Secura
A BUREAU VERITAS COMPANY

RAPPORT

Scenario's en maatregelen voor cyberweerbare zonnestroominstallaties

Publicatieversie

TLP: CLEAR

AUGUSTUS 2024

Secura BV | +31 (0)88 888 31 00 | info@secura.com | secura.com

BUREAU VERITAS

Deze rapportage is opgesteld door Secura in opdracht van de Rijksdienst voor Ondernemend Nederland, op verzoek van en in samenwerking met de Topsector Energie (Programma Digitalisering en TKI Urban Energy).

TLP: CLEAR*

Augustus 2024

*Het Traffic Light Protocol (TLP) is een standaard die wordt gebruikt om aan te duiden wanneer en op welke wijze informatie mag worden verspreid. TLP:CLEAR betekent dat dit document, onder voorbehoud van de regels op het gebied van auteursrechten, onbeperkt en publiekelijk kan worden verspreid (met inachtneming van de toepasselijke voorschriften en procedures voor openbaarmaking van informatie). Voor meer informatie zie de website van het Nationaal Cyber Security Centrum.

Inhoudsopgave

1. Over dit onderzoek

Zonnestroom wordt een steeds groter deel van de totale Nederlandse energievoorziening. Vooral op zonnige zomerdagen is het aandeel van stroom uit zonnestroominstallaties enorm. Daarmee wordt echter ook de Nederlandse afhankelijkheid van een stabiele toelevering van deze zonnestroom steeds groter. Het is dan ook cruciaal dat deze stabiele toelevering niet plots verstoord kan worden door bijvoorbeeld een cyberaanval. Zodoende is er vanuit RVO (Rijksdienst voor Ondernemend Nederland) de samenwerking gezocht met topsector energie (energie experts) en Secura (cybersecurity experts) om een onderzoek op het vlak van cybersecurity in de zonnesector uit te voeren.

Gedurende dit onderzoek is de zonnestroomsector in detail bekeken. Het doel was om een concreet beeld van het aanvalsoppervlak en de mogelijke dreigingen te krijgen. Vervolgens werd bepaald wat de vermoedelijke impact zou zijn wanneer deze dreigingen werkelijkheid werden. Uiteindelijk werd er daarna gezocht naar mitigerende maatregelen om dergelijke aanvallen te voorkomen of de impact ervan te reduceren. Daarbij werd de nadruk gelegd op welke entiteit deze maatregelen zou kunnen nemen.

Om de benodigde informatie op tafel te krijgen voor de onderzoekers is er gebruik gemaakt van een combinatie van open bronnen, gesloten bronnen, verdiepingsinterviews met experts uit de sector en een klankbordgroep van verschillende afgezanten van organisaties werkzaam in de sector. De resultaten van dit onderzoek zijn tijdens het onderzoek herhaaldelijk ter review aangeboden aan de verschillende experts om er zeker van te zijn dat de juiste informatie overgebracht werd.

Het onderzoek heeft geleid tot 27 scenario's die kunnen leiden tot grootschalige verstoring van de zonnestroomsector. Daarnaast is geconstateerd dat dergelijke verstoringen ook effect zullen hebben op de gehele energiesector en dat sommige scenario's ook effecten zullen hebben buiten de zonnestroomsector.

Hoewel over de kans van een succesvolle aanval gediscussieerd kan worden, is de potentiële impact van deze scenario's desastreus te noemen. Er is veelal sprake van grote economische schade, fysieke schade en zelfs maatschappelijke schade. Zeker wanneer de secundaire gevolgen van de cyberaanval ook meegenomen worden.

Om deze scenario's te voorkomen en de impact ervan te verkleinen zal door vrijwel alle entiteiten in de zonnesector actie ondernomen moeten worden. Denk daarbij aan ingrijpen vanuit overheid, maar ook vanuit brancheorganisaties, installateurs, zonnestroominstallatie-fabrikanten, consumentenbonden en de individuele consument. Iedereen heeft een rol in de totale cyberweerbaarheid van het stroomnet, geen van de entiteiten is in staat om dit vanuit hun positie zelf volledig op te lossen. Dit wordt voornamelijk veroorzaakt door de toenemende complexiteit en connectiviteit binnen de sector en het binnen stroomnet in het algemeen.

De geleerde lessen tijdens dit onderzoek zullen gedeeltelijk ook buiten de zonnesector relevant zijn of overeenkomen met conclusies uit onderzoeken op andere sectoren, zoals de elektrische-voertuigsector of de batterijsector.

Omdat het onderzoek relatief snel erg complex werd en veel terminologie bevatte is ervoor gekozen om twee documenten te publiceren. Het eerste document is een publiek document, dat bedoeld is voor het algemeen publiek en niet al te veel terminologie en details bevat. Daarnaast is er een tweede document met "Technische achtergrond" beschikbaar voor personen die de materie op detailniveau willen doornemen en volledig willen begrijpen hoe en waarom de betreffende conclusies getrokken zijn.

2. Introductie

2.1. Algemene introductie onderzoek

Rijksdienst voor Ondernemend Nederland (RVO) en Topsector Energie hebben een verkenning laten uitvoeren naar cybersecuritysamenwerking en kennisdeling in de zonne-energiesector (TNO, 2024). Uit deze verkenning bleek dat het risico op verstoring van zonnestroominstallaties door cyberincidenten reëel is. Tevens bleek, dat het aannemelijk is dat er door middel van cyberaanvallen op de zonne-energiesector verstoringen veroorzaakt kunnen worden in de elektriciteitsvoorziening. Dit onderzoek leverde een aantal vervolgvragen op: Waar zitten dan de grootste cybersecurityrisico's? Wat is de impact wanneer er misbruik gemaakt wordt van deze zwakheden? En hoe kunnen deze risico's verkleind worden? Zodoende kwam dit vervolgonderzoek, gericht op het beantwoorden van deze vragen.

Doel van het onderzoek

Het primaire doel van dit onderzoek is het beantwoorden van de ontstane vervolgvragen uit de eerdere verkenningsfase om op die manier het volgende in kaart te brengen: waar de zwakke plekken rondom zonnestroom vermoedelijk zitten, wat er zou kunnen gebeuren en wat er gedaan zou kunnen worden om dit tegen te gaan.

Het secundaire doel van dit onderzoek is het verhogen van het bewustzijn en duidelijk maken welke rollen de verschillende stakeholders (zouden moeten) hebben om de cyberweerbaarheid van de zonnesector als geheel te verbeteren.

Scope van het onderzoek

De scope van het onderzoek betreft Nederlandse zonnestroominstallaties, in de context van de Nederlandse positie in de Europese energiemarkt, en diens geopolitieke verhoudingen. Er wordt daarbij een onderscheid gemaakt tussen:

- Residentieel op dak (<15kWp), kleinschalig
- Grootschalig op dak (bijvoorbeeld school/boerderij/bedrijventerrein)
- Zonneparken (>1MW)

Omdat de zonnestroominstallaties een onderdeel zijn van het grotere energielandschap, zullen een aantal van de uitkomsten van het onderzoek vermoedelijk ook van toepassing zijn op andere sectoren, zoals windenergie, laadpalen voor elektrische auto's, batterijsystemen, enzovoorts. De nadruk van dit onderzoek licht echter op de rol die zonnestroom in dit geheel speelt.

2.2. Onderzoeksvragen en methodologie

Onderzoeksvragen

- Wie zijn de potentiële aanvallers (dreigingsactoren)? Wat is hun motivatie?
- Wat is het belangrijkste aanvalsoppervlak van de zonne-energiesector? Wat zijn logische aanvalspaden om de zonne-energiesector middels een cyberaanval te raken?
- Wat zou de (realistische) impact van een dergelijke aanval kunnen zijn?
- Wat zijn de mogelijke oplossingen om de kans of de gevolgen van zo'n aanval te verkleinen?

Methodologie

Gedurende een periode van 6 maanden hebben de onderzoekers informatie verzameld, door het raadplegen van openbare en gesloten bronnen (bijvoorbeeld hackersfora op het *darkweb*), interviews en groepssessies met stakeholders en vak-experts uit de (zonne-)energie en cybersecuritysector. Deze informatie is vervolgens verwerkt in dit onderzoeksrapport. De betreffende geïnterviewde personen en aanwezigen bij de groepssessies hebben gedurende deze periode herhaaldelijk de mogelijkheid gehad om het onderzoeksrapport te reviewen en eventuele fouten aan te merken voor verbetering. Voor verdere details omtrent de gehanteerde methodologie kunt u terecht in het technische achtergrond document.

2.3. Leeswijzer

Dit document is de publieke versie van het onderzoek. Dit document is bedoeld om goed leesbaar te zijn voor personen die niet diep in de betreffende materie thuis zijn en toch de betreffende conclusies willen begrijpen. Bepaalde details zijn achterwege gelaten om de leesbaarheid te bevorderen.

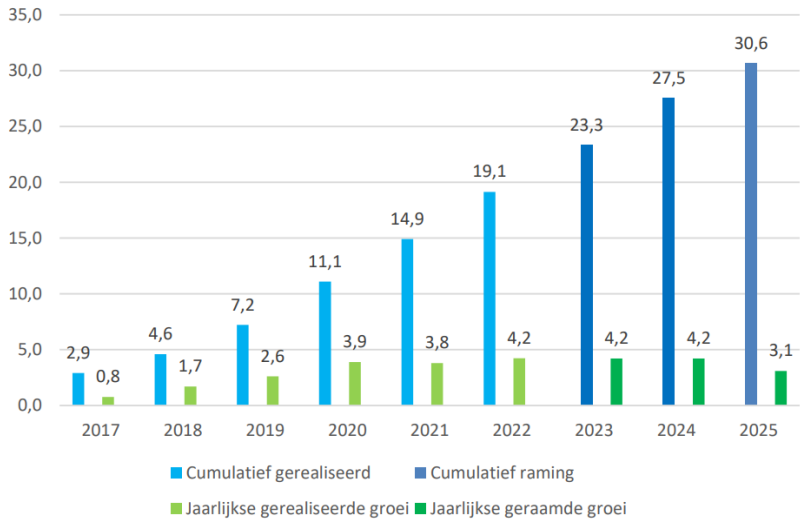
Naast deze publieke versie is er ook een technisch achtergronddocument (Secura, 2024). Dit technische achtergronddocument is bedoeld voor vakinhoudelijke experts die bekend zijn met de relevante terminologie en bevat de details van het gehele onderzoek. We raden experts aan om eerst de publieke versie te lezen en vervolgens waar nodig de diepgang op te zoeken in het technische achtergronddocument.

Het technisch achtergronddocument is uitgebracht onder TLP:GREEN, wat betekent dat de informatie niet publiekelijk beschikbaar is maar gedeeld wordt met organisaties in de energiesector of met dezelfde doelstellingen respectievelijk informatiefora of personen werkzaam in de netwerkbeveiliging en/of informatiebeveiliging. Het achtergronddocument kan worden opgevraagd via een formulier op de Topsector Energie website, te vinden op: https://topsectorenergie.nl/kennisbank/maatregelen-cyberveiligheid-zonpv/.

3. Context

3.1. Achtergrondinformatie

Zonne-energie is een steeds belangrijker onderdeel van de energiemix in Nederland en in Europa. Het totaal opgestelde vermogen groeit ieder jaar flink en inmiddels staan er meer dan 3 miljoen zonnestroominstallaties in Nederland. In totaal is er op dit moment zo'n 27,5 GW aan geïnstalleerd vermogen. In de praktijk leverden die zonnepanelen in 2023 zo'n 17GW op aan het stroom netwerk (Dutch New Energy Research en Solar 365, 2024). In de vroege zomerdagen van 2024 zien we deze piek zelfs toenemen naar zo'n 20GW. Dit verschil ontstaat doordat niet alle zonnepanelen hun volledige vermogen leveren, door de verschillende ligging van de panelen.



Figuur 1: Opbrengst zonnestroom
(https://www.rijksoverheid.nl/documenten/rapporten/2023/10/09/monitor-zon-pv-2023-in-nederland)

Van het totale vermogen aan zonnestroom wat opgewekt wordt, komt zo'n 57% uit de zonneparken en grootschalige installaties op daken en zo'n 43% uit kleinschalige installaties, veelal op daken van huizen. Daardoor kunnen we stellen dat naast de zonneparken ook de kleinschalige installaties een belangrijke rol spelen in de zonne-energiesector.

Binnen Nederland wordt op dit moment SolarEdge als marktleider gezien van zonnestroom omvormers. Daarnaast spelen Huawei, SMA, GoodWe, Fronius en Enphase een grote rol. In de statistieken is echter ook te zien dat in recente jaren met name omvormers van Aziatische afkomst (bijvoorbeeld Huawei en SunGrow) het grootste deel van de Nederlandse markt in handen hebben gekregen. Door die grote afhankelijkheid zou je kunnen stellen dat we met de huidige energietransitie als het ware overgaan van Russisch gas naar een afhankelijkheid van "Chinese stroom".

Uit eerder onderzoek (TNO, 2024) is gebleken dat het risico op verstoringen van zonnestroominstallaties door cyberincidenten reëel is. Daarnaast zijn er verschillende zorgelijke trends geïdentificeerd (TNO, 2024) waardoor ingeschat wordt dat het risico voor deze sector (en de energiesector in het algemeen) steeds groter in plaats van kleiner wordt en dat de kans op serieuze schade veroorzaakt door cyberincidenten toeneemt. Tevens is bekend dat stroomstoringen op kleine of grote schaal altijd significante problemen met zich meebrengen omdat Nederland afhankelijk is van stroom voor nagenoeg alle facetten van het dagelijks leven.

De zonnesector zelf heeft een groot aantal betrokken entiteiten en door verschillende partijen geproduceerde componenten. Al deze entiteiten en componenten spelen een bepaalde rol in de cyberweerbaarheid van het geheel. Juist doordat er zoveel componenten en entiteiten zijn die een rol spelen in deze sector is het erg moeilijk om goed grip te krijgen op de werkelijke risico's en wie er een rol kan (of zou moeten) spelen om deze risico's te verkleinen. Dit onderzoek heeft daarom als doel om voor alle relevante partijen duidelijker in kaart te brengen welke rol zij in het geheel (zouden moeten) spelen en waarom het zo belangrijk is dat ze dat doen.

3.2. PV-landschap

Hoewel een zonnestroominstallatie op het eerste gezicht relatief simpel lijkt, is dit vanuit een cybersecurity perspectief en het stroomnet perspectief anders. Hieronder lichten we een aantal cruciale en veelvoorkomende componenten en hun rol in het PV-landschap (PV staat voor '*Photovoltaïc*' oftewel zonne-energie.) toe. Voor een meer gedetailleerd overzicht kan gekeken worden in de "Doelen en aanvalsoppervlak" sectie in het technische achtergronddocument.

Component	Relevantie voor de zonnesector
Zonnepanelen	Dit zijn de panelen die op het dak leggen en de daadwerkelijke stroom opwekken. De zonnepanelen zelf zijn geen slimme apparaten.
Omvormer	Dit is het apparaat dat de opgewekte stroom van de zonnepanelen omzet naar stroom die geschikt is voor het lokale stroomnet. Daarnaast is dit veelal het hart van de zonnestroominstallatie. Het is zodoende ook uitgerust met diverse manieren om te communiceren met bijvoorbeeld Cloud systemen, mobiele apparaten en andere omliggende systemen.
Hardwarecomponenten	Dit zijn de componenten in de omvormers, denk aan computerchips, die vaak standaard worden ingekocht. Kwetsbaarheden die de betreffende standaard chip raken, kunnen dan dus ook de zonnestroominstallatie raken waar deze inzitten.
Cloud-portalen van fabrikanten	Veel zonnestroominstallaties worden gekoppeld aan het internet, sturen hun data naar de Cloud en kunnen aangestuurd worden vanuit de Cloud. Op deze manier hebben personen waar ook ter wereld controle over de installaties. In sommige gevallen kunnen installaties ook aan een installateur toegewezen worden, die op deze manier op afstand de functionele werking van het apparaat kan monitoren.
Mobiele applicaties	Vanuit gebruiksvriendelijkheid en de wens van de gebruiker om te kunnen zien hoeveel stroom opgewekt wordt, hebben veel partijen mobiele applicaties gemaakt die interacteren met de PV-installatie (in veel gevallen via de cloud-dienst).
Aansluiting op het stroomnet	Iedere zonnestroominstallatie is op een manier gekoppeld aan het stroomnet. Hoe dit precies gebeurt en met welke materialen is bepalend voor eventuele risico's.
HEMS	HEMS staat voor Home Energy Management System. Dit is als het ware een computer die een aantal apparaten in een huis slim aan kan sturen. Zo kan een dergelijk systeem bijvoorbeeld aan de hand van de dynamische energieprijs besluiten om de elektriciteit van de zonnepanelen te gebruiken om terug te leveren als de prijs hoog is of juist lokaal te gebruiken om bijvoorbeeld een elektrische auto op te laden als de prijs laag is.
Batterij	Het gebeurt steeds vaker dat bij een zonnestroominstallatie ook een batterij geplaatst wordt. Deze batterijen zorgen ervoor dat de opwek van de installatie gedurende de dag ook gebruikt kan worden wanneer het donker wordt. Ook worden dergelijke batterijen regelmatig ingezet in '*virtual powerplants*' om in te spelen op de verschillende energiemarkten en om het net in balans te houden.
Centrale markten	Er zijn diverse "stroommarkten". Hier wordt stroom middels vraag en aanbod verhandeld. Zo kan er bijvoorbeeld op de congestiemarkt verzocht worden door de hoogspanningsbeheerder om geen stroom te leveren op een piektijd voor een

	bepaald bedrag per KWh. Andersom kan er ook gevraagd worden om juist stroom te leveren op een bepaalde tijd voor een bepaald bedrag. Op deze manier wordt er met de dynamische actuele prijs ad hoc gehandeld in leveringscontracten. Een contractbreuk heeft grote boetes tot gevolg. Naast de congestiemarkt zijn er nog andere centrale markten waar een vergelijkbaar handelsproces plaats vindt.
Installateurs/beheerders monitoring	Diverse installateurs of beheerders bieden een monitoring dienstverlening aan. Soms plaatsen ze hiervoor zelf apparatuur om op afstand het apparaat te kunnen monitoren en soms zelfs aan kunnen sturen. Anderen maken gebruik van “installateurs” functionaliteiten die geboden worden door Cloud-portalen van de maker van de omvormer en monitoren op die manier op afstand de installatie.
Veiligheidseisen PV	Veel van de componenten die gebruikt worden in zonnestroominstallaties moeten voldoen aan specifieke veiligheidsstandaarden. Dit komt omdat in het verleden al bewezen is dat niet voldoen dergelijke standaarden en instructies van de PV-fabrikant kan leiden tot brandgevaar en elektrocutie. Dergelijke standaarden nemen over het algemeen geen cybersecurity-eisen mee, ook al lijkt het in sommige gevallen wel mogelijk om via cyberaanvallen de veiligheidsparameters te beïnvloeden.
Lokale netwerk en omliggende systemen	Residentiële zonnestroom installaties zijn meestal aan het lokale Wi-Fi netwerk of bekabelde netwerk aangesloten. De veiligheid van dit netwerk en de apparaten in dat netwerk kunnen bepalend zijn voor het risico op cybersecurity-incidenten in de zonnestroominstallatie.
Financiële prikkels	Er zijn diverse subsidieregelingen om de energietransitie te versnellen door gebruik van bepaalde systemen aan te moedigen. Gedreven door o.a. deze prikkels ontwikkelt de zonne-energiesector zich snel. In de praktijk wordt meestal alleen de prijs van de installatie gebruikt in vergelijkingen, waardoor soms kwalitatief slechtere of minder veilige systemen in grote getalen geplaatst worden.
Slimme energiemeters	De slimme meter houdt bij hoeveel stroom er afgenomen en terug geleverd wordt aan het net.
Zekeringen en spanningsbeveiligingen	Iedere residentiële stroomaansluiting heeft een zekering en spanningsbeveiliging. Dit zit voor een groot deel in de meterkast, maar daarnaast zijn er ook nog grotere zekeringen die bij grote hoeveelheden stroom zorgen dat de elektrische installatie uitschakelt.

Voor zonneparken of grotere installaties specifiek zijn daarnaast ook de volgende componenten nog relevant:

Component	Relevantie voor de zonnesector
Eigen spanningsbeveiliging inclusief blindvermogen controle	Grote zonneparken hebben ook een sterkere spanningsbeveiliging nodig, deze dienen de parkeigenaren zelf te installeren. Daarnaast moet een dergelijk systeem ook monitoren op het zogenoemde “blind vermogen” omdat dit op langere termijn schade en warmteproblematiek kan veroorzaken.
Monitoring via dataloggers	Een andere manier om te verbinden met een intern monitoringsysteem en beheerportaal is via dataloggers. Deze apparaten krijgen informatie van de zonnestroominstallatie over de actuele opwek en sturen dit door naar centrale monitoringssystemen. In sommige gevallen kunnen deze monitoringssystemen ook gebruikt worden om de zonnestroominstallaties aan te sturen. Deze systemen zijn veelal ‘*read-only*’, maar hebben ook hun eigen aanvalsoppervlak in de vorm van bijvoorbeeld een web interface.
EMS	Grote zonneparken worden regelmatig ook gecombineerd met windturbines en batterijsystemen. Al deze systemen samen worden vervolgens via het Energie Managementsysteem (EMS) centraal aangestuurd. Dergelijke systemen zijn lokaal opgesteld en kunnen via die weg met de zonnepanelen installaties communiceren,

	maar worden door de energieleverancier op afstand veelal via cloud-connecties en cloud-portalen aangestuurd.
Fysieke beveiliging	Met fysieke toegang tot het zonnepark kan eenvoudig schade toegebracht worden aan installaties of een apparaat geplaatst worden, die op een later moment ingezet kan worden om een cyberaanval uit te voeren. Daarom zijn er veelal hekken en camera's aanwezig.
Remote operatie	Vaak is er in zonneparken een manier om op afstand apparaten aan te sturen. Soms gebeurt dat via een EMS maar andere keren door een beveiligde remote toegangsmogelijkheid of een cloud-applicatie waar de lokale systemen aan gekoppeld zijn.
Leverancierstoegang	Om de goede werking van het zonnepark te garanderen is er vaak op afstand monitoring en support mogelijk. Via deze weg kunnen de leveranciers van de apparatuur op afstand de systemen beheren om storingen op te lossen.
Curtailment verzoeken van de netbeheerder (veelal via een RTI)	RTI staat voor Real Time Interface. Dergelijke systemen zijn verplicht voor alle grotere zonneparken. Dit systeem zorgt ervoor dat de regionale netbeheerder informatie krijgt over het zonnepark. Daarnaast kan de netbeheerder een verzoek sturen dat vrijwel altijd automatisch opgevolgd wordt, om bijvoorbeeld minder stroom te produceren. Een RTI moet altijd een gecertificeerd product zijn, zodoende zijn er slechts een klein aantal aanbieders van dit product.
Acquisitie zonneparken door buitenlandse partijen	Het gebeurt regelmatig dat buitenlandse investeerders Nederlandse zonneparken aankopen. Zij worden daarmee onderdeel van het Nederlandse stroomnet. Hierdoor krijgen andere landen controle en rechten over stukjes vitale infrastructuur van Nederland.

4. Dreigingsactoren

In de wereld bestaan verschillende personen of groepen die allemaal hun eigen motivatie kunnen hebben om de zonnesector aan te vallen. Een dergelijke persoon of groep noemen we in de cybersecuritywereld een “dreigingsactor”. De motivatie of het achterliggende doel van zo’n dreigingsactor om de zonnesector aan te vallen kan significant verschillen. Ook de middelen die een dreigingsactor heeft kunnen heel anders zijn. Zo heeft een door de overheid gesponsorde hackersgroep van 50 personen een stuk meer financiële middelen, tijd en technische capaciteit beschikbaar dan mogelijk activistische actoren of individuen.

Gedurende het onderzoek zijn de volgende ‘dreigingsactoren’ naar voren gekomen als potentiële aanvallers van de zonnesector:

Dreigingsactor	Primaire drijfveer	Relevantie voor de zonnesector
Georganiseerde misdaad	Financieel gewin	Dreigingsanalyses uit 2023 (NCTV, ENISA) laten zien dat de energiesector als geheel op de radar staat bij ransomware groepen. Hier valt de zonnesector ook onder. Het is daarbij dan ook niet ondenkbaar dat ransomware groepen zich op verstoring van kritieke infrastructuur gaan richten om zo grote losgeldbedragen te verkrijgen. De zonnesector is hier gevoeliger voor dan andere sectoren, vanwege het toenemende aantal connecties en aantal afhankelijkheden van andere systemen.
Statelijke actoren	Spionage, mogelijkheid op disruptie	Omdat de zonnesector onderdeel is van de kritieke infrastructuur is deze sector interessant voor statelijke actoren, met het oog op kleinschalige of grootschalige verstoring. Binnen de zonnesector specifiek is de dreiging vanuit de statelijke actoren relatief groot omdat het een eenvoudige route naar verstoring mogelijk maakt. Statelijke actoren kunnen bijvoorbeeld een bedrijf dat firmware voor omvormers maakt dwingen een backdoor voor hen in te bouwen of het bedrijf verzoeken controle over remote aansturingsfaciliteiten aan de statelijke actor over te dragen. Er ontstaat op dat moment voor Nederland een strategische afhankelijkheid van deze statelijke actor omdat deze de vitale infrastructuur van Nederland kan raken. Dit kan bijvoorbeeld als pressiemiddel gebruikt worden in geopolitieke onderhandelingen. Daarnaast wordt er veel geld verdiend met de verkoop van zonnepaneleninstallaties en is diefstal van intellectueel eigendom een interessante mogelijkheid om de eigen economie te versterken.
Onethische bedrijven	Financieel gewin, concurrentie voordeel	Door cyberaanvallen op leverende systemen (en voorkennis wanneer deze cyberaanvallen plaats gaan vinden) kan een onethisch bedrijf de energiemarkt beïnvloeden om op die manier de bedrijfswinst flink te verhogen. Daarnaast zou een dergelijk bedrijf ook via cyberaanvallen de opwekkende systemen van een concurrent kunnen beïnvloeden. Op die manier zou de concurrent reputatieschade en significante economische schade toegebracht worden en het bedrijf zelf een concurrentievoordeel verkrijgen.
Hacktivisten	Aandacht voor ideologische missie	Hacktivisten zijn gedreven door de geopolitiek of door maatschappelijke onderwerpen. Zo zijn er diverse voorbeelden (Counter threat unit research team, 2023) van een bedrijf dat wereldwijd componenten levert en aangevallen wordt omdat het van origine uit een bepaald land komt, waartegen de hacktivisten in kwestie morele bezwaren heeft.
Individuen	Sterk wisselend	Er zijn altijd individuen die een persoonlijke reden hebben om een bepaald bedrijf of een bepaalde sector aan te vallen. Dit kan bijvoorbeeld nieuwsgierigheid zijn, financiële prikkels, of wraak willen nemen na een

		conflict met de werkgever. Hoewel de kundigheid en mogelijkheden per individu sterk kunnen verschillen kunnen deze persoonlijk gemotiveerde aanvallen tot serieuze incidenten leiden. De impact blijft echter veelal beperkt tot de getroffen organisatie.
Overig	Schade aanrichten	Onder deze categorie vallen vandalen en terroristen. Op dit moment wordt deze categorie niet als relevant gezien voor de zonnesector, omdat een cyberaanval veelal geen passend middel is voor de doelen en motivaties van dergelijke actoren. Deze beoordeling zou echter in de toekomst zeker kunnen veranderen wanneer zich incidenten voordoen.

5. Wat is er in het kort mogelijk

In deze sectie lichten we toe welke systemen rondom PV-installaties geraakt zouden kunnen worden door een cyberaanval en wat dat naar verwachting voor gevolgen zou hebben. Voor de volledige technische achtergrond over hoe en waarom dergelijke zaken mogelijk zijn en welke componenten het dan exact betreft verwijzen we u graag naar het technische achtergronddocument. Ter illustratie zijn er in de navolgende secties een aantal mogelijke scenario's in detail uitgewerkt.

5.1. Wat kan er aangevallen worden?

Residentieel en klein zakelijk aanvalsoppervlak

Door heel Nederland heen zijn kleine PV-installaties op daken van woonhuizen en kleine bedrijven. Dergelijke installaties bestaan vaak uit 6 tot 20 zonnepanelen en 1 omvormer en leveren een kleine hoeveelheid vermogen. Als je al deze kleine vermogens echter bij elkaar optelt betreft het huidige cumulatieve vermogen van deze kleine installaties naar schatting (Gastel, 2024) meer dan 10GW. Een hack op een enkele installatie is weliswaar vervelend voor de eigenaar, maar heeft verder weinig impact. Wanneer er echter een aanval op grote schaal mogelijk is, is de impact wel significant.

Binnen de categorie residentieel en klein zakelijk aanvalsoppervlak werden in totaal 12 schaalbare scenario's geïdentificeerd die op grote en middelmatige schaal zonnestroominstallaties kunnen raken.

Aanvalsoppervlak van grootzakelijke installaties en zonneparken

Hoewel alle scenario's die voor residentiële en klein zakelijke zonnepanelen installaties van toepassing zijn ook van toepassing zijn op grootzakelijke zonnepanelen installaties en zonneparken, is er daarnaast een aantal aanvullende scenario's denkbaar. In totaal werden er naast de 12 schaalbare scenario's nog 15 aanvullende scenario's geïdentificeerd die alleen van toepassing zijn voor grootzakelijke installaties en zonneparken.

Al met al zijn er dus 27 scenario's opgesteld die een serieuze impact op de zonnesector en de stabiliteit van de energiesector in algemene zin te hebben. In dit document zijn een drietal scenario's in nader detail uitgewerkt in sectie 6, 7 en 8. Voor een exact overzicht van de scenario's verwijzen we u graag naar de sectie "Overzicht van aanvalsscenario's" in het technische achtergronddocument.

5.2. Wat gebeurt er als zoiets aangevallen wordt?

Wat er precies gebeurt tijdens een werkelijke cyberaanval is natuurlijk moeilijk te zeggen. Het hangt ook af van welke dreigingsactor op welk moment welke aanval uitvoert. Maar op hoofdlijnen zijn de volgende zaken te voorzien.

Economische schade

Een zonnestroominstallatie levert geld op. Bij iedere verstoring is er dan ook sprake van enige economische schade omdat er geen stroom meer opgewekt wordt. Op grotere schaal zoals bijvoorbeeld bij zonneparken kan deze schade flink oplopen.

Daarnaast hebben zonneparken of virtuele zonneparken (een groot aantal kleine installaties bij elkaar) vaak afspraken over hoeveel stroom ze aanleveren op enig moment. Wanneer zij zich niet aan deze afspraken houden (ondanks mogelijke overmacht), kunnen er forse boetes opgelegd worden door de netbeheerder.

Ook is het denkbaar dat een cyberaanval bepaalde componenten van de zonnestroom-installatie tijdelijk of zelfs permanent beschadigt. Deze componenten zullen vervangen moeten worden, wat de nodige financiële kosten met zich meebrengt. Daarnaast zal, wanneer dit op grotere schaal gebeurt, de levertijd van dergelijke componenten en de beschikbaarheid van installateurs een sterk beperkende factor zijn. Daardoor kan de economische schade verder oplopen, vanwege boetes en niet opgewekte stroom. In specifieke gevallen zouden ook omliggende apparaten in het lokale stroomnet zoals televisies, telefoons, waterkokers etc. beschadigd kunnen raken en vervangen moeten worden. De kans hierop is niet groot en vereist specifieke configuratie door de aanvaller, maar is door zaken als piekspanning wel mogelijk.

Naast de rechtstreekse economische schade is er ook indirecte schade mogelijk. Wanneer de stroom op kleine of grotere schaal uitvalt zijn er veel zaken niet meer mogelijk of aanzienlijk moeilijker. Winkels kunnen niet meer pinnen waardoor er minder omzet wordt gedraaid, of fabrieken staan stil waardoor er geen productie meer gedraaid wordt. Afhankelijk van hoelang deze stroomuitval duurt en op welke schaal dit plaats vindt heeft dit een relatief geringe tot significante financiële consequenties.

Fysieke schade

Zoals eerder benoemd is er een reële kans dat door een cyberaanval componenten van de zonnestroom-installatie permanent beschadigd raken. Deze componenten zullen fysiek vervangen moeten worden door installateurs. Daarnaast zal eventuele beschadigde omliggende apparatuur ook fysiek vervangen moeten worden. Dit kan veelal door de consument of bedrijfseigenaar zelf uitgevoerd worden. De vraag daarbij is echter wel waar de uiteindelijke rekening van dergelijke beschadigde apparatuur terecht komt en tot in hoeverre dit bijvoorbeeld via verzekeringen of via installateurs/stroomleveranciers te verhalen is.

Uit eerdere gevallen (NOS, 2015) is bekend dat ten tijde van stroomuitval er allerlei andere maatschappelijke problemen ontstaan. Zo vallen er bijvoorbeeld veel beveiligingssystemen uit waardoor er meer misdaden gepleegd worden, kunnen grote hoeveelheden gekoelde producten bedorven raken omdat koeling uitvalt of gebeuren er meer ongelukken omdat verkeersregelinstallaties uitgevallen zijn.

Daarnaast is het niet ondenkbaar dat door een hack elektrische parameters van de zonnepaneleninstallatie dusdanig aangepast worden dat er een verhoogd brandrisico ontstaat. Of dit daadwerkelijk tot een brand leidt is afhankelijk van een groot aantal factoren, denk daarbij aan de interne beveiliging van de omvormer en hoeverre deze zijn aan te passen en het verdere ontwerp van de omvormer. Maar ook zaken als waar het apparaat geplaatst is en wat er omheen staat of op ligt, welke kabels en afsluitdoppen er gebruikt zijn door de installateurs, welke apparaten zich in het lokale stroomnet bevinden en hoe brandveilig die zijn, etc. (TNO, 2019). Het is voor een aanvaller niet mogelijk een specifieke installatie of aangesloten specifiek apparaat brand te laten veroorzaken. Maar wanneer veel systemen tegelijk geraakt worden door een cyberaanval is het niet uit te sluiten dat er door reeds aanwezig omstandigheden brand kan ontstaan. TNO spreekt in hun onderzoek van een percentage van 0,014% van de installaties waar brand kan ontstaan door de contextuele factoren (meestal gebrekkige bekabeling). Als je dus 100 000 systemen in Nederland zou raken zouden er naar verwachting 14 van die geraakte installaties brand kunnen veroorzaken. In de context van een cyberaanval waarbij de elektrische parameters aangepast worden kan dit percentage mogelijk iets toenemen.

Schade aan het stroomnet

Het stroomnet is een complex geheel dat constant bewaakt wordt en altijd in balans moet blijven. Het is namelijk belangrijk dat er net zoveel stroom afgenomen wordt als er opgewekt wordt. Kleine fluctuaties daarin zijn wel mogelijk, maar deze moeten niet te groot worden, anders ontstaan er serieuzere problemen zoals stroomstoringen. Een aanval op zonnepanelen zou een dergelijke kleine of grote fluctuatie mogelijk kunnen maken.

Laagspanningsnet: klein risico
Op laagspanningsniveau (een gebied gekoppeld aan een transformatorhuis, denk aan bijvoorbeeld een woonwijk of bedrijventerrein) heeft het wegvallen van de zonnestroom naar verwachting geen tot zeer geringe impact op het stroomnet. Het wegvallen wordt direct gecompenseerd door toelevering vanuit het midden- en hoogspanningsnet waardoor er ook geen cascade effecten op andere omliggende zonnepanelen installaties zijn. Wel is het mogelijk, met name op zonnige dagen, om een teveel aan zonnestroom te creëren. Dit kan door manipulatie van de grenswaarden waarop de omvormers zouden moeten uitvallen. Hierdoor zou er een zekering in het laagspanningsstation kunnen uitvallen, met als gevolg een kleine lokale storing die relatief snel te repareren is.

Het is daarnaast mogelijk om de elektrische parameters van de omvormer zo te beïnvloeden dat er weliswaar geen directe schade optreedt maar een versnelde veroudering van de apparatuur in de laagspanningsstations optreedt. Op welk moment het laagspanningsstation dan precies uitvalt door het kapotgaan van een van de onderdelen is niet in te schatten. De storing zal naar verwachting wel langer duren omdat er een cruciaal onderdeel onverwacht kapotgegaan is. Vanuit (een klein aantal) residentiële systemen is hier geen noemenswaardig effect te verwachten. De meeste zonneparken monitoren hier actief op en kunnen systemen uitzetten als de gemeten waarden te veel afwijken.

Midden- en hoogspanningsnet: groter risico
Om echt significante gevolgen voor het stroomnet te hebben moet het midden- en hoogspanningsnet geraakt worden. De stabiliteit daarvan wordt echter gegarandeerd door alle samenwerkende partijen in Europa. Hierdoor is een specifieke aanval op Nederland onwaarschijnlijk. De kans is groter dat een dergelijke aanval zich op heel Europa richt. Binnen Europa is er zo'n 3 GW aan noodvermogens beschikbaar om bijvoorbeeld een storing op te vangen. Wanneer fluctuaties groter worden dan dat, kunnen er stroomstoringen ontstaan en worden er crisismaatregelen genomen, met als uiterste noodmaatregel het afschakelen van regio's.

In Nederland is in 2023 zo'n 24 GW (CBS, 2024) aan zonnestroom geïnstalleerd. Rekening houdend met zaken als installatie hoek en hoeveelheid zonlicht is in de zomermaanden de maximale opwekking in alleen Nederland in 2023 geschat op zo'n 16,6 GW voor Juni 2024 wordt dit geschat op 19,4GW (Energie Opwek, 2024). Dit zou betekenen dat op een zonnige dag in 2023, 18% van alle zonne-energie in Nederland weg zou moeten vallen om op die 3GW uit te komen. Op dit moment zijn er een tweetal omvormerfabrikanten (Huawei, Sungrow) die zo'n groot marktaandeel in Nederland hebben dat een aanval op alleen de systemen van die fabrikant voldoende zou kunnen zijn om deze drempelwaarde te bereiken. Op winterse dagen leveren de zonnepanelen in Nederland niet genoeg vermogen om deze drempel te halen. De verwachting (Sluijters, 2022) is dat in geheel Europa in 2025 zo'n 327,6 GW en in 2030 zo'n 672GW geïnstalleerd vermogen zal staan. Meerdere fabrikanten zouden in heel Europa, zelfs op minder zonnige dagen, over die drempelwaarde komen. Een aanval gericht op Europa als geheel is daarom dus waarschijnlijker dan een aanval op specifiek Nederland.

De theoretische drempelwaarde van 3GW zou mogelijk ook eerder al gehaald kunnen worden door in te spelen op de markten. Door gecoördineerd een tegengestelde actie te doen dan wat er door de markt gevraagd wordt (bijvoorbeeld door veel meer stroom leveren i.p.v. minder) kan de drempelwaarde sneller behaald worden. Ditzelfde geldt ook voor het op grote schaal manipuleren van elektrische parameters van omvormers. Hoe meer systemen er simultaan geraakt worden, hoe moeilijker er nog te compenseren valt.

Zeker wanneer een dergelijke aanval ook nog gecombineerd zou worden met een aanval op andere sectoren die een grote invloed hebben op het stroomnet, zoals windenergie, batterij-opslagsystemen, EMS-systemen en laadpalen is een grootschalige stroomstoring een aannemelijk scenario. Ook als een grootschalige storing uitblijft omdat de drempelwaarde niet voldoende overschreven is, resulteert de inzet van noodvermogen wel in grote financiële schade. Het inzetten van noodvermogen is namelijk erg duur.

Ook het op grote schaal leveren van zonne-energie terwijl dit niet de bedoeling is zou kunnen leiden tot overbelasting, waardoor regionaal zekeringen of beveiligingsrelais kapot kunnen gaan. Hierdoor kunnen regionale stroomstoringen ontstaan.

Maatschappelijke schade

De combinatie van bovenstaande zaken heeft serieuze gevolgen voor de Nederlandse maatschappij. Allereerst is er een serieus risico op kleinschalige, regionale of zelfs grootschalige landelijke stroomuitval met alle indirecte gevolgen van dien die alle inwoners raken.

Wanneer de hierboven beschreven incidenten zich voor zouden doen kan dat in meer of mindere mate voor maatschappelijke onrust of zelfs geopolitieke onrust zorgen. De secundaire gevolgen van (langdurige) stroomuitval moeten daarbij niet onderschat worden. In de zogeheten piramide van Maslow (behoeftepiramide van de mens) wordt uitgelegd dat de behoeften van de mens zich gelaagd ontwikkelen. Pas als aan de voorwaarden aan de onderkant van de piramide (grotendeels) voldaan wordt, kan de volgende laag bereikt worden. De secundaire gevolgen van (langdurige) stroomuitval raken echter de onderste 3 lagen van deze behoefte piramide en raken de slachtoffers in hun lichamelijke behoeften (bijv. geen eten kunnen kopen door pinstoringen, koelkasten en vriezers die niet langer werken), veiligheid en zekerheid (verhoogd brandrisico, onzeker wanneer zaken weer gaan werken, toename van criminaliteit, gebrek aan mogelijkheid tot hulp krijgen) en sociaal contact (digitale communicatie middelen niet langer beschikbaar of functioneel). Een dergelijke verstorende situatie kan veel stress en ongewoon gedrag bij burgers met zich meebrengen.

Ook kan een dergelijke aanval het vertrouwen in zonnestroom beschadigen. Hierdoor zal de bereidheid om daarin te investeren afnemen en de energietransitie mogelijk vertragen. Ook zal er ten tijde van de cyberaanval en het oplossen van deze aanval tijdelijk weinig tot geen zonnestroom gebruikt worden en teruggegrepen moeten worden naar fossiele bronnen wat een negatieve invloed heeft op het klimaat. Ter vergelijking, de grootste gascentrale in Nederland heeft ongeveer 1,3GW vermogen (Wikipedia, 2024). Om een verlies van zo'n 25% van de zonnepanelen in Nederland op te vangen zullen er dus ongeveer 4 van deze centrales op maximaal vermogen stroom moeten gaan leveren. Mede door de geleidelijke afbouw van fossiele brandstoffen in deze tijd van energietransitie is de vraag of we ten tijde van zo'n aanval nog wel kunnen terugvallen op fossiele bronnen of dat we hier dan de capaciteit niet meer voor hebben.

Verdienmodel voor kwaadwillenden

Met het aanvalsoppervlak in gedachten en de daaropvolgende potentiële impact, is het goed denkbaar dat criminelen op enig moment geld zullen proberen te verdienen aan deze sector. Allereerst is het mogelijk om bedrijven of personen te chanteren en te dreigen met stroomuitval, schade aan installaties, datalekken etc. Daarnaast is ook een ransomware-achtig model denkbaar, waarbij de systemen onklaar gemaakt worden tot er betaling plaatsvindt.

Ook is het niet ondenkbaar dat er intellectueel eigendom buitgemaakt wordt bij de verschillende spelers in de energiemarkt die vervolgens te koop wordt aangeboden aan andere partijen die dezelfde markt proberen te bedienen. Daarnaast zou, gegeven de theoretische maatschappelijke impact, de toegang tot systemen verkocht kunnen worden aan statelijke actoren om op die manier de mogelijkheid te krijgen om de vitale infrastructuur van Nederland of Europa als geheel te raken. Hierdoor ontstaat er een afhankelijkheid van deze statelijke actor voor Nederland of Europa die onwenselijk is en gebruikt kan worden om bepaalde geopolitieke keuzes te beïnvloeden.

Als laatste zijn zonnepaneleninstallaties zelf ook interessant als '*botnet*' (een groep van systemen die vanuit een centraal punt aangestuurd kunnen worden om opdrachten uit te voeren), simpelweg omdat het apparaat in staat is om acties uit te voeren voor de *botnet*-eigenaar, er veel van zijn, ze een netwerkkoppeling hebben, en de beveiliging doorgaans slecht is.

Details

In het technische achtergronddocument is gedetailleerd beschreven wat de exacte impact is voor eigenaren en voor het stroomnet wanneer de beschikbaarheid, integriteit of vertrouwelijkheid van zonnepaneleninstallaties op kleine of grote schaal geraakt wordt. Om de lezer een concreter beeld te geven van wat er echt mis kan gaan in de zonnesector zijn in de volgende secties een aantal fictieve scenario's beschreven. Deze scenario's zijn gebaseerd op werkelijke aanvallen die verspreid over de wereld reeds hebben plaatsgevonden.

6. Scenario 1: aanval via webportalen

Wat gebeurt er?

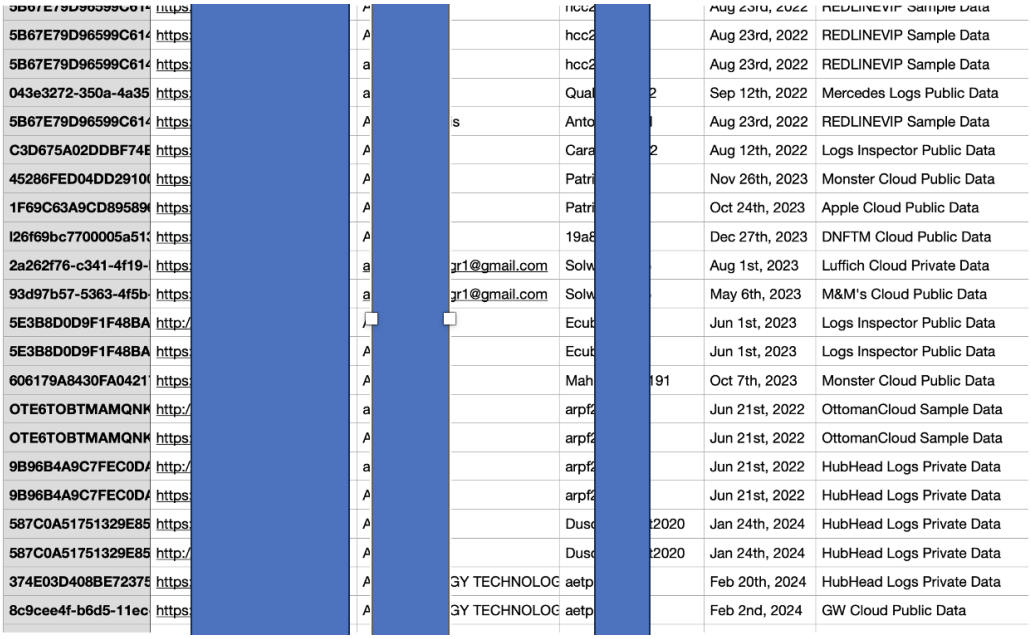
Een cyber-criminele ransomware bende ziet een opportunistische kans om beheerders van zonneparken af te persen. Door gestolen wachtwoorden op het *darkweb* te kopen en kwetsbaarheden te vinden in Cloud-platformen van fabrikanten, worden meerdere accounts van grote installateurs overgenomen.

Met deze accounts weet een aanvaller de beschikking te krijgen over beheerfunctionaliteit van duizenden residentiële en grotere zonnestroominstallaties. De zonneparkbeheerders worden via een onbekend mailadres gechanteerd om een groot bedrag in bitcoin te betalen. Wanneer dit niet gebeurt zullen de cybercriminelen de installaties beschadigen of ervoor zorgen dat de organisatie zich niet aan de leveringsafspraken kan houden door manipulatie van de apparaten. Als bewijs dat het geen bluf is, wordt een klein aantal systemen al onklaar gemaakt. Er moet binnen 4 uur betaald worden. Ook geven de criminelen aan dat enige poging om de hackers uit het systeem te werken zal resulteren in het beschadigen van alle bereikbare installaties.

Op advies van de politie wordt er niet betaald en wordt er een poging gedaan om zo veel mogelijk systemen af te koppelen. Het afkoppelen wordt echter opgemerkt door de cybercriminelen, omdat zij de verbinding met een aantal installaties verliezen. Vervolgens configureert de cyber-criminele bende via de daarvoor bedoelde functionaliteiten in het portaal alle nog bereikbare apparaten anders. Door enkele parameters in de configuratie van omvormers te wijzigen (zoals power-factor, output voltage en drempelwaardes voor afschakelen) worden eerste enkele, en vervolgens duizenden installaties beschadigd. Ook veel apparatuur die op dezelfde lokale stroomvoorziening is aangesloten wordt beschadigd of ontregeld door de veroorzaakte elektrische problemen.

Waar ligt de kern van dit probleem?

In dit scenario speelt de beveiliging van de centrale portalen een grote rol. Het verkrijgen van wachtwoorden door cybercriminelen is voor hen al lang geen probleem meer, aangezien dergelijke bendes al veel langer malware schrijven om wachtwoorden te stelen en deze te verkopen op het *darkweb*. Het is dan ook gebleken uit een rondgang door de portalen van diverse fabrikanten dat talloze (honderden tot duizenden) accountgegevens (gebruikersnamen en wachtwoorden) van installateurs en eindgebruikers in datadumps voorkomen en op het *darkweb* te koop staan. In het verleden zijn dergelijke accountgegevens ook al per ongeluk (Security.nl, 2022) voor het algemeen publiek beschikbaar geweest via *github*.



5B67E79D96599C614	https	[redacted]	A	[redacted]	hcc2	[redacted]	Aug 23rd, 2022	REDLINEVIP Sample Data
5B67E79D96599C614	https	[redacted]	a	[redacted]	hcc2	[redacted]	Aug 23rd, 2022	REDLINEVIP Sample Data
043e3272-350a-4a35	https	[redacted]	a	[redacted]	Quat	[redacted]2	Sep 12th, 2022	Mercedes Logs Public Data
5B67E79D96599C614	https	[redacted]	A	[redacted]s	Anto	[redacted]	Aug 23rd, 2022	REDLINEVIP Sample Data
C3D675A02DDBF74E	https	[redacted]	A	[redacted]	Cara	[redacted]2	Aug 12th, 2022	Logs Inspector Public Data
45286FED04DD2910(	https	[redacted]	A	[redacted]	Patri	[redacted]	Nov 26th, 2023	Monster Cloud Public Data
1F69C63A9CD89589(	https	[redacted]	A	[redacted]	Patri	[redacted]	Oct 24th, 2023	Apple Cloud Public Data
l26f69bc7700005a51	https	[redacted]	A	[redacted]	19a8	[redacted]	Dec 27th, 2023	DNFTM Cloud Public Data
2a262f76-c341-4f19-	https	[redacted]	a	[redacted]gr1@gmail.com	Solw	[redacted]	Aug 1st, 2023	Luffich Cloud Private Data
93d97b57-5363-4f5b	https	[redacted]	a	[redacted]gr1@gmail.com	Solw	[redacted]	May 6th, 2023	M&M's Cloud Public Data
5E3B8D0D9F1F48BA	http:/	[redacted]	A	[redacted]	Ecut	[redacted]	Jun 1st, 2023	Logs Inspector Public Data
5E3B8D0D9F1F48BA	https	[redacted]	A	[redacted]	Ecut	[redacted]	Jun 1st, 2023	Logs Inspector Public Data
606179A8430FA0421	https	[redacted]	A	[redacted]	Mah	[redacted]191	Oct 7th, 2023	Monster Cloud Public Data
OTE6TOBTMAMQNK	http:/	[redacted]	a	[redacted]	arpf2	[redacted]	Jun 21st, 2022	OttomanCloud Sample Data
OTE6TOBTMAMQNK	https	[redacted]	A	[redacted]	arpf2	[redacted]	Jun 21st, 2022	OttomanCloud Sample Data
9B96B4A9C7FEC0D/	http:/	[redacted]	a	[redacted]	arpf2	[redacted]	Jun 21st, 2022	HubHead Logs Private Data
9B96B4A9C7FEC0D/	https	[redacted]	A	[redacted]	arpf2	[redacted]	Jun 21st, 2022	HubHead Logs Private Data
587C0A51751329E85	https	[redacted]	A	[redacted]	Dusc	[redacted]t2020	Jan 24th, 2024	HubHead Logs Private Data
587C0A51751329E85	http:/	[redacted]	A	[redacted]	Dusc	[redacted]t2020	Jan 24th, 2024	HubHead Logs Private Data
374E03D408BE7237	https	[redacted]	A	[redacted]GY TECHNOLOG	aetp	[redacted]	Feb 20th, 2024	HubHead Logs Private Data
8c9cee4f-b6d5-11ec	https	[redacted]	A	[redacted]GY TECHNOLOG	aetp	[redacted]	Feb 2nd, 2024	GW Cloud Public Data

Figuur 2: Voorbeelden van inloggegevens van centrale portalen in datadumps en op het darkweb Q1 2024.

Hierbij is het van belang op te merken dat dergelijke portalen vaak niet de mogelijkheid bieden tot sterke beveiliging (goede versleuteling, multifactor authenticatie etc.) of wanneer ze dit aanbieden het gebruik daarvan niet afgedwongen wordt. Een aanvaller die enige tijd accounts verzamelt zal in staat zijn om een significante hoeveelheid zonnepaneleninstallaties aan te sturen. Het is echter moeilijk om vooraf vast te stellen waar deze omvormers zich precies bevinden. Een gerichte aanval op specifiek Nederland is daarmee minder waarschijnlijk, maar niet onmogelijk. Met name installateurs- of beheerderaccounts zijn relatief eenvoudig aan Nederlandse bedrijven te koppelen, al helemaal als .nl email adressen gebruikt zijn.

Wat zijn de gevolgen voor de eindgebruikers?

De gevolgen van dit scenario zullen vooral merkbaar zijn voor de individuele eindgebruikers, omdat hun installaties onbruikbaar worden en schade veroorzaken aan andere apparatuur in huis of in het bedrijfspand. Dit kan in specifieke gevallen mogelijk zelfs tot veiligheidsissues en een verhoogd brandgevaar leiden. Deze gevolgen zullen ongetwijfeld leiden tot verzekeringsclaims en een grootschalig beroep op de installateurs om de omvormers te vervangen, met lange wachttijden en leveringsproblemen als gevolg.

Daarnaast zijn er natuurlijk ook economische gevolgen voor het niet produceren van zonnestroom (van kleine schaal thuis gebruiker tot grotere schaal zonnepark). Voor de partijen die meedoen op de energiemarkt kan dit niet produceren ook tot mogelijke boetes leiden voor het niet nakomen van productie contracten.

Voor een meer gedetailleerde uitleg zie ook Sectie “Potentiële gevolgen” in het technische achtergronddocument.

Wie had dit kunnen voorkomen?

Omdat de accounts van de installateurs en gebruikers een belangrijke schakel zijn in het aanvalspad, zal de verantwoordelijkheid allereerst bij deze partijen liggen om het probleem te verhelpen. Onder meer door het wijzigen van wachtwoorden, het instellen van meerstapsverificatie waar mogelijk, en het

oplossen van de gevolgen door het herstellen van de parameters van de systemen en het (laten) repareren van beschadigde componenten en apparaten.

In tweede instantie ligt er echter ook een verantwoordelijkheid bij de fabrikant van de portalen en de PV-installaties. De beveiligingsmaatregelen in zowel de PV-installatie als in de portalen zijn immers tekortgeschoten. Zo had er bijvoorbeeld multifactorauthenticatie afgedwongen kunnen worden voor de accounts in het portaal. Of had er bij het wijzigen van elektrische parameters een vier ogen-principe moeten zijn, waarbij de installateur de actie kan initiëren, maar de systeemeigenaar deze wel eerst moet goedkeuren voordat deze daadwerkelijk doorgevoerd wordt.

Daarnaast zouden de '*failsafes'* van de PV-installatie voor de elektrische veiligheid moeten voldoen aan alle veiligheidseisen in de Europese en lokale wetgeving. Toch is er als onverwacht gevolg van de cyber aanval een klein aantal branden ontstaan en is er schade aan omliggende apparatuur veroorzaakt. De vraag daarbij is dan ook: hoe kan het dat ondanks de garantie van elektrische veiligheid dit toch gebeurd is en wie is er aansprakelijk voor het feit dat er toch een veiligheidsprobleem opgetreden is? (Denk hierbij aan een installateur die componenten onjuist geplaatst heeft of verkeerde kabels gebruikt heeft waardoor er een dakbrand ontstaan is. Of een consument die zijn kast met de omvormer tevens gebruikt als oud papier-opslag van zijn bedrijf, waardoor de hitte van het apparaat het papier heeft laten vlamvatten etc.)

Wat zijn de gevolgen voor anderen?

Ook de beheerders van zonneparken zullen gevolgen ondervinden. Zij zijn immers degenen die in dit scenario worden afgeperst. Criminelen bewijzen in het algemeen eerst dat ze impact kunnen veroorzaken. Om betaling van het 'losgeld' waarschijnlijk te maken is het bijvoorbeeld mogelijk dat ze wachten op een zonnige dag, om vervolgens aan te tonen dat ze de accounts hebben overgenomen van in totaal enkele honderden megawatt aan productiecapaciteit en daarmee schade aan kunnen richten.

Hoewel de zonneparkbeheerders hier de afgeperste partij zijn, zijn zij niet de enige slachtoffers en bovendien niet de partij die er iets aan kan doen om het probleem op te lossen. Dit maakt de gevolgen voor hen erg lastig in te schatten. Het is van belang dat zijvoldoende contacten onderhouden met fabrikanten en eindgebruikers, en hen helpen bij het oplossen van het probleem. Uiteindelijk zou het gevolg kunnen zijn dat zonneparkbeheerders het losgeld betalen om ergere of kostbaardere problemen te voorkomen.

Op technisch vlak is een mogelijk gevolg dat de portalen en accounts waar het om gaat tijdelijk niet meer beschikbaar zijn, omdat de fabrikanten die de portalen onderhouden deze uitzetten om verdere aanvallen te voorkomen. Dit zou uiteraard gevolgschade kunnen hebben voor alle (ook niet gehackte) eigenaren, omdat deze niet langer gebruik kunnen maken van het portaal.

Voor de stroomproductie van de zonnepaneleninstallatie zelf, heeft dit niet per se directe gevolgen, tenzij de aanvaller bewust de stroomproductie probeert te beïnvloeden. De stroomproductie kan wel geraakt worden wanneer er specifiek Energie Management Systeem-portalen of centrale online markten onbeschikbaar gemaakt worden. Er kan dan namelijk niet meer goed ingespeeld worden op vraag en aanbod en beschikbare capaciteiten omdat die informatie niet langer beschikbaar is. Het wordt daardoor lastiger om te produceren (het kan nog steeds met behulp van lokale aansturing, dit is echter niet in alle gevallen mogelijk). Hierdoor neemt de kans op netcongestie of balansproblemen in het algehele stroomnet toe.

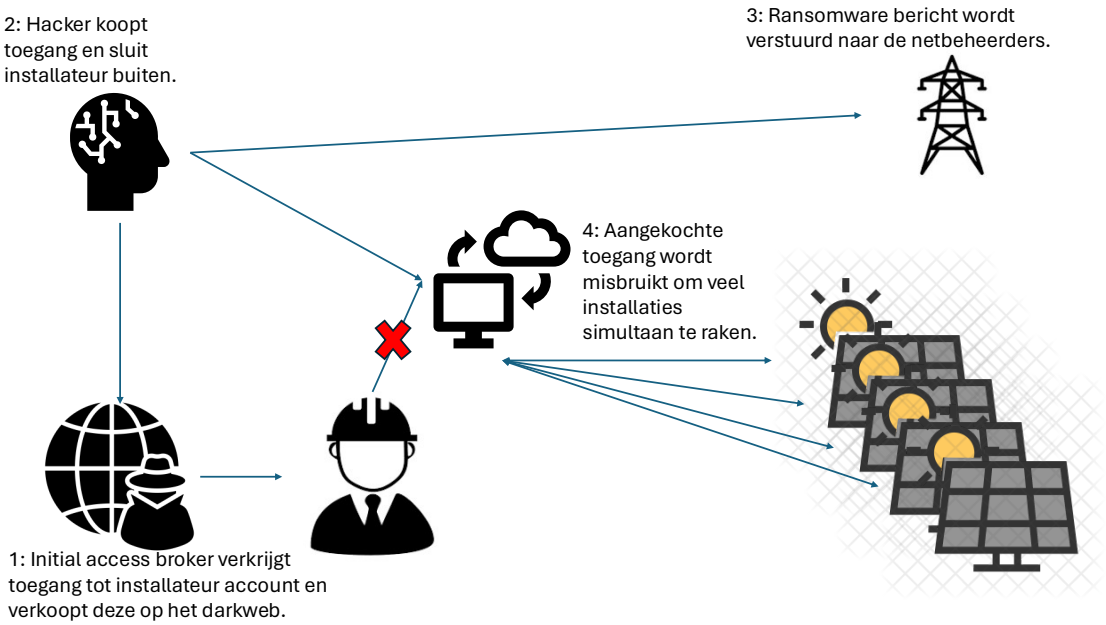
Eigenaren van (met name grote) installaties zouden ook alle remote verbindingen (VPN-routers, blokkeren van verkeer naar cloud-portalen e.d.) uit kunnen zetten om verdere aanvallen te voorkomen. Het resultaat van een dergelijke aanval zal daarom zeer waarschijnlijk betekenen dat grote delen van de zonnestroominstallaties preventief of voor onderhoud uit wordt gezet, met significante economische en ecologische schade tot gevolg.

Daarnaast hebben op de langere termijn de verhalen in de media over verhoogd brandgevaar en omliggende apparatuur die beschadigd is geraakt door een hack op de zonnepaneleninstallatie een negatief effect. De bereidwilligheid om een dergelijke installatie te plaatsen zal afnemen wat de energietransitie mogelijk verder vertraagt.

Voor een meer gedetailleerde uitleg zie ook sectie “Potentiële gevolgen” in het technische achtergronddocument.

Schematische weergave

Niet iedere dreigingsactor zal met hetzelfde doel een aanval op een webportaal uitvoeren. De stappen in de aanval zijn echter voor het overgrote deel hetzelfde, ongeacht de motivatie. Hieronder volgt een versimpelde schematische weergave van dit scenario.



Figuur 3: Schematische weergave van een mogelijke aanval via een webportaal

Voorbeeldscenario omzetten naar maatregelen

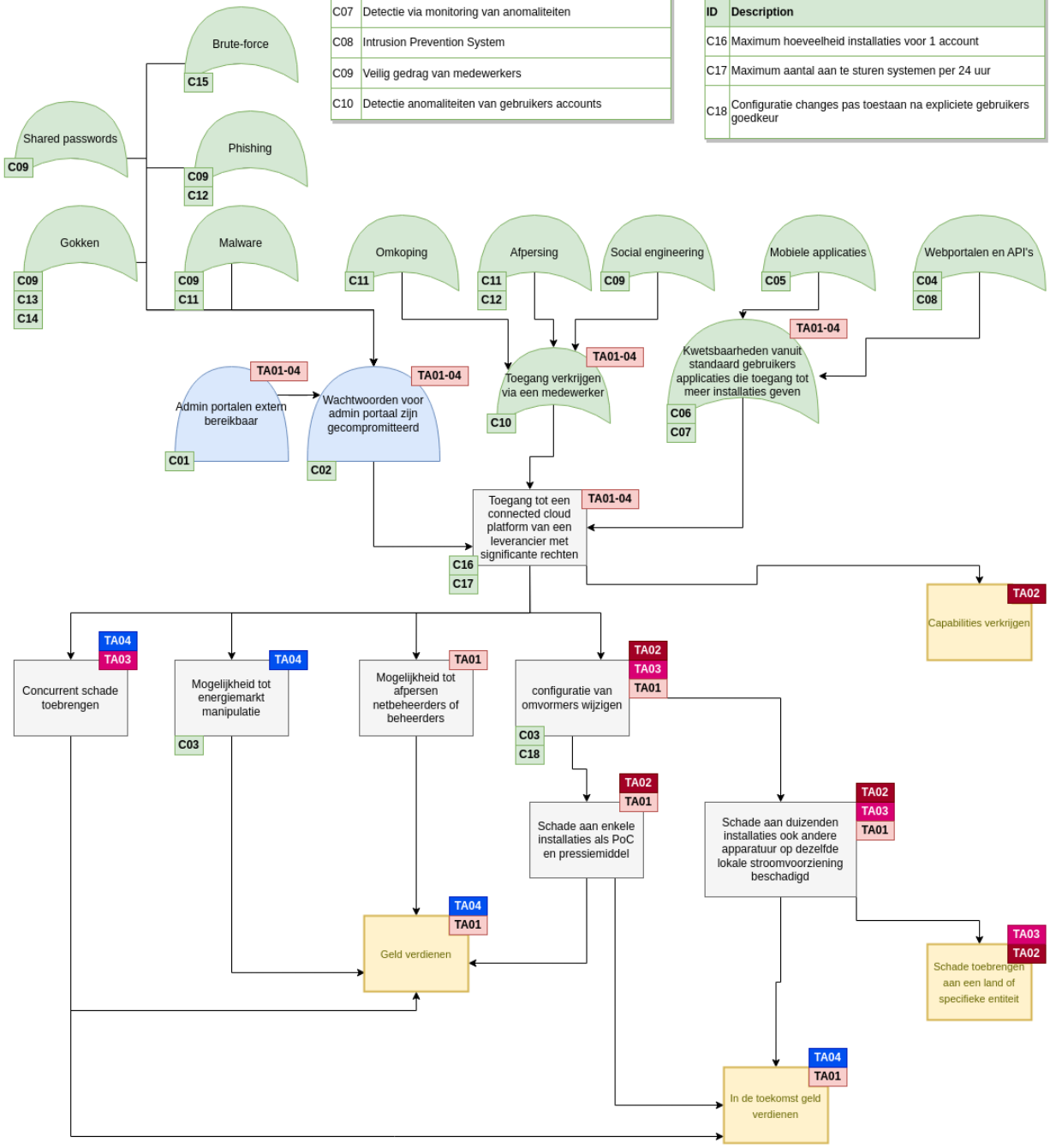
Scenario’s zoals deze kunnen gebruikt worden om te bepalen welke maatregelen verstandig zijn om te nemen. Om een voorbeeld te geven van hoe je dat zou kunnen doen is er een zogenaamde “attack tree” op de volgende pagina toegevoegd. Een dergelijke grafische weergave van mogelijke paden om tot een bepaald scenario en de mogelijke gevolgen te komen kan helpen bij het uitdenken van de benodigde tegenmaatregelen.

Threat Actors	
ID	**Description**
TA01	Georganiseerde misdaad
TA02	Statelijke actoren
TA03	Hacktivist
TA04	Onethische bedrijven

Security Controls Preventief en detectief deel 1	
ID	**Description**
C01	IP whitelisting
C02	2FA implementation
C03	Technically enforced 4 eye principle
C04	ASVS normen toepassen voor development
C05	MASVS normen toepassen voor development
C06	Pentesting
C07	Detectie via monitoring van anomaliteiten
C08	Intrusion Prevention System
C09	Veilig gedrag van medewerkers
C10	Detectie anomaliteiten van gebruikers accounts

Security Controls Preventief en detectief deel 2	
ID	**Description**
C11	Endpoint protection system
C12	Mail filters, Externe mail waarschuwingen
C13	Sterk wachtwoord beleid
C14	Zwarte lijst voor gelekte wachtwoorden
C15	Anti-automatiserings maatregelen

Security Controls impact verkleinend	
ID	**Description**
C16	Maximum hoeveelheid installaties voor 1 account
C17	Maximum aantal aan te sturen systemen per 24 uur
C18	Configuratie changes pas toestaan na expliciete gebruikers goedkeur



Figuur 4: Voorbeeld van een attack tree met bijbehorende actoren en mogelijke mitigerende maatregelen

7. Scenario 2: Omvormers overnemen

Wat gebeurt er?

Een omvormerfabrikant merkt dat personen regelmatig problemen hebben om het systeem succesvol aan de cloud-omgeving te koppelen. Daarom wordt er een firmware update uitgebracht die bij de eerste installatie tijdelijk een extra poort openzet naar het publieke internet. Zo kan er vanuit de fabrikant rechtstreeks verbinding gemaakt worden om het systeem alsnog aan de cloud te koppelen. In de praktijk blijkt echter dat deze poort, die alleen tijdelijk open zou moeten staan op niet verbonden omvormers, permanent open staat op alle omvormers met deze nieuwe firmware. Achteraf blijkt dit een fout in de programmacode van de firmware.

Het gevolg is dat tienduizenden omvormers met een standaard wachtwoord, dat bij installatie niet gewijzigd is, worden overgenomen. Binnen twee dagen blijken cybercriminelen een 'bot' te gebruiken die de omvormers overneemt en inlijft in een *botnet*. Dit *botnet* voert DDoS-aanvallen uit en installeert crypto-mining software. Tegelijkertijd misbruiken hacktivistische groepen hetzelfde lek om de omvormers over te nemen, maar dan om hun geopolitieke activistische boodschap uit te dragen of apparaten van specifieke fabrikanten aan te vallen.

Dit alles zorgt ervoor dat steeds meer systemen niet meer kunnen worden benaderd. Ze blijven in de meeste gevallen wel functioneren, maar de bediening op afstand, datacommunicatie met de mobile app of cloud werken niet meer. Het vereist een handmatige en fysieke interventie om te worden hersteld.

Dit scenario is een combinatie van eerder voorgekomen situaties. Kwetsbaarheden in interfaces van zonnepaneleninstallaties die aan het internet gekoppeld waren werden misbruikt door het Mirai *botnet* en werden vervolgens gebruikt voor financieel gewin (Brumfield, 2024). In een ander voorbeeld heeft een fabrikant 800.000 micro-omvormers in één dag, op afstand, van een nieuwe update voorzien om bepaalde problemen op te lossen (Fairley, 2015) . Ook heeft een eerder onderzoek van het RDI (Rijksinspectie Digitale Infrastructuur, 2023) aangetoond dat wanneer een omvormer bereikbaar is voor een kwaadwillende, het vaak mogelijk is om de omvormer over te nemen. De recente aanval van anti-Israëlische hacktivisten op PLC-systemen (Counter threat unit research team, 2023) is ook een recent voorbeeld van opportunistisch hacktivisme wat ook Nederland kan raken ondanks dat Nederland niet het directe doelwit is.

Figuur 5: Voorbeeld van Hacktivistische overname van Nederlandse apparatuur

Waar ligt de kern van dit probleem?

Dit probleem is in essentie complex. Het is een samenloop van omstandigheden waarbij verschillende actoren actie hadden kunnen ondernemen. Systemen die aan het internet gekoppeld zijn liggen altijd en iedere dag onder vuur. Er zijn diverse entiteiten die dag en nacht het gehele internet scannen op zoek naar kwetsbare systemen. Daarom zou een systeem pas aan het publieke internet gekoppeld moeten

worden (zelfs als dit maar tijdelijk is) na een serieuze risicoafweging en mogelijk zelfs na een cybersecuritytest.

In dit specifieke voorbeeld wordt de fout in de firmware onbewust geïntroduceerd. Het is echter ook denkbaar dat dergelijke achterdeuren bewust aangebracht worden door bepaalde dreigingsactoren Er zouden dan ook tegenmaatregelen getroffen moeten worden om dit tegen te gaan. Denk daarbij aan zaken als een technisch afgedwongen vier ogen-principe op het uitbrengen van nieuwe firmware, het niet simultaan updaten van alle apparatuur, maar hiervoor een gefaseerde aanpak in hanteren, of zelfs het open source maken van firmware zodat onafhankelijke partijen hier onderzoek naar kunnen doen en aan bij kunnen dragen.

Wat zijn de gevolgen voor de eindgebruikers?

De individuele gevolgen voor eindgebruikers zullen niet groot zijn, maar het herstellen van een dergelijke aanval zal zeer moeilijk zijn, omdat veel omvormers zullen moeten worden vervangen of ten minste handmatig moeten worden voorzien van nieuwe firmware. Ook hiervoor moeten installateurs op pad om systemen te vervangen of repareren.

Mede door het feit dat fysieke interventie lastig is om grootschalig uit te voeren, blijven veel apparaten langdurig kwetsbaar. Een nieuwe veilige firmware zal niet overal (even snel) geïnstalleerd worden. Het is dan ook gebleken dat dergelijke *botnets* erg lang kunnen blijven bestaan. Het Mirai *botnet* (Cloudflare, 2024) stamt uit 2016, en bestaat (in gewijzigde vorm) nog steeds in 2024. Het herstellen van een dergelijke botnetaanval zal dus waarschijnlijk nooit helemaal succesvol zijn.

Wie had dit kunnen voorkomen?

De primaire veroorzaker van dit probleem is de omvormer fabrikant geweest. De fout in de programmalogica had mogelijk voorkomen kunnen worden door zaken als een vier ogen-principe voor het uitrollen van een update, een beter risicoafwegingsproces en het meenemen van cybersecurity-eisen bij het testen van de firmware op een representatieve testopzet voor zowel bestaande als nieuwe te plaatsen systemen. Daarnaast hadden er ook een aantal *best practices* rondom firmware-bescherming genomen kunnen worden.

De daadwerkelijke exploitatie en inlijving bij het *botnet* had ook voorkomen kunnen worden door het wijzigen van het standaard wachtwoord. Maar een competente aanvaller had wellicht ook andere kwetsbaarheden kunnen vinden in de plots beschikbare interfaces, zoals in het verleden vaker gebleken is uit security-onderzoeken op omvormers (Rijksinspectie Digitale Infrastructuur, 2023).

Er ligt echter ook een verantwoordelijkheid bij de installateurs en gebruikers, die in veel gevallen het standaard wachtwoord niet hebben gewijzigd. Daarmee was de aanval aanzienlijk moeilijker geworden of in schaal afgenomen. Ook hier had de omvormer fabrikant een rol kunnen spelen door het wijzigen van het standaard wachtwoord technisch af te dwingen of multifactorauthenticatie toe te passen op de inlogmogelijkheid. Ook hadden met name zakelijke of professionele organisaties zelf omliggende mitigerende maatregelen kunnen nemen in het eigen netwerk, zoals firewalling, geen permanente verbinding hebben met het update-portaal, monitoring van afwijkingen in het netwerkverkeer etc.

De conclusie is dus dat in dit scenario meerdere actoren dit probleem hadden kunnen voorkomen. De primaire stimulans daarbij ligt echter bij de omvormer fabrikant omdat deze waarschijnlijk te maken krijgt met de grootste reputatieschade. De installateurs hebben enerzijds de stimulans om hun werk goed te doen (mogelijk ook gestuurd door omvormer fabrikant richtlijnen) maar anderzijds krijgen zij meer werk op het moment dat ze op veel plekken de systemen opnieuw moeten plaatsen.

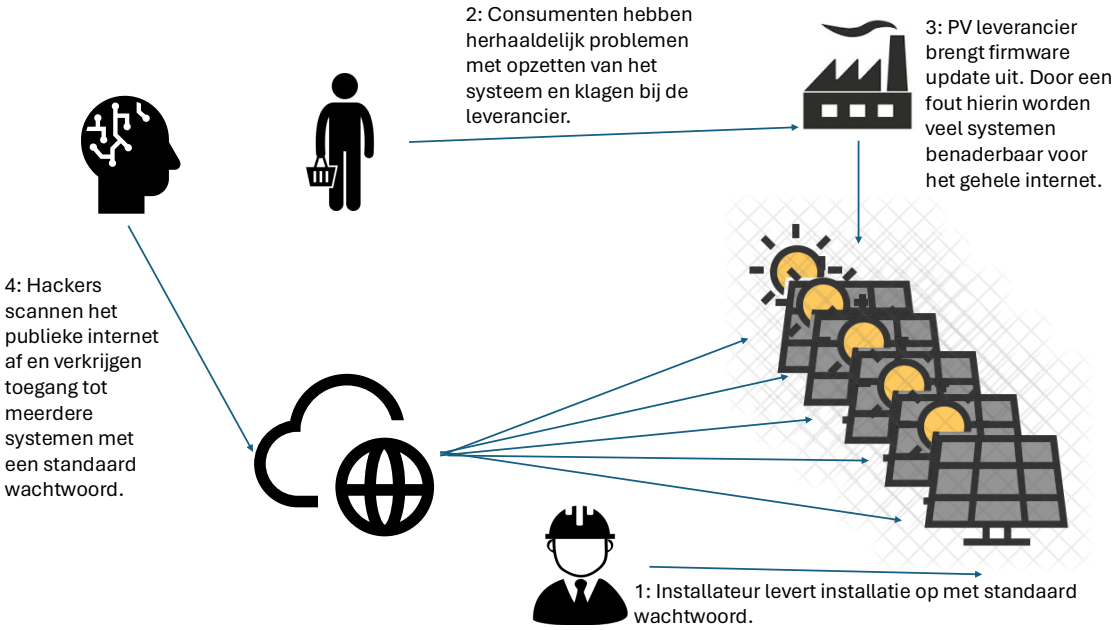
Wat zijn de gevolgen voor anderen?

Netbeheerders zullen geen of weinig directe gevolgen ondervinden omdat de stroomopwekking actief blijft en er niet geknoeid wordt met de energieparameters. Wel is te verwachten dat een dergelijke situatie imagoschade voor de hele zonnesector zal veroorzaken. Waarschijnlijk ontstaat er ook wel enige maatschappelijke onrust, die eventueel de energietransitie kan afremmen.

Ook is het bestaan van een *botnet* onprettig voor de maatschappij als geheel omdat deze ingezet kan worden voor zaken als DDoS aanvallen, waar verschillende partijen last van kunnen hebben.

Schematische weergave

Niet iedere dreigingsactor zal met hetzelfde doel een aanval vanaf het publieke internet zoals eerder geschetst uitvoeren. Het publieke internet wordt echter 24/7 gescand door verschillende actoren. Een dergelijke fout wordt extreem snel misbruikt. Hieronder volgt een versimpelde schematische weergave van dit scenario.



Figuur 6: Schematische weergave van het ontstaan van scenario 2.

8. Scenario 3: Supply-chain aanval

Wat gebeurt er?

Naarmate de geopolitieke spanningen door de verschillende gaande oorlogen oploopt, besluiten verschillende landen ieder voor zich om de mogelijkheden te gaan vergaren om kritieke infrastructuur via cyberwapens uit te schakelen. Een van deze statelijke actoren besluit zich op de zonnesector te richten en voert een supply-chain aanval uit door het firmware-update mechanisme te compromitteren. Vervolgens wordt er een achterdeur in de nieuwe firmware van een sub-component geplaatst. Dit type sub-component wordt veel in grootschalige zonneparken gebruikt. Door deze achterdeur kan op een willekeurig moment op een later tijdstip volledige controle over de zonneparken en grote aantallen omvormers worden verkregen.

Wanneer de situatie escaleert besluit het land in kwestie dit cyberwapen te activeren. Door het manipuleren van elektrische parameters van de omvormers ontstaan op landelijke en zelfs Europese schaal verstoringen. Het snel op- en afschakelen van productiecapaciteit kan niet tijdig worden gevolgd door opvang van noodvoorzieningen. Het gevolg: een grootschalige black-out.

Dit scenario is gebaseerd op de bewezen kennis en kunde van buitenlandse mogendheden (Advanced Persistent Threats, of APT's). Van diverse landen met een offensief cyber-programma is het bekend zij dat dergelijke supply-chain aanvallen kunnen voorbereiden en uitvoeren. Daarnaast wordt opgemerkt dat het zeker niet ondenkbaar is dat ook criminele groeperingen een dergelijke aanval zouden kunnen uitvoeren, als ze daartoe de mogelijkheid zien (opportunistisch). Het is minder waarschijnlijk dat de georganiseerde misdaad een dergelijke supply-chain aanval vooraf zal bedenken, plannen en uitvoeren.

Het is waarschijnlijk dat een statelijke actor zich niet alleen op Nederland maar op heel West-Europa zou richten. Het aanvalsoppervlak van bijvoorbeeld Duitsland, waar zonnestroominstallaties veel talrijker zijn, is vele malen groter. Daarbij is het Nederlandse hoogspanningsnetwerk sterk verweven met dat van andere landen in Europa. De impact van een aanval op andere landen in Europa zou, vanwege die afhankelijkheden, zeker tot in Nederland voelbaar zijn, en misschien zelfs grotere gevolgen hebben dan een aanval op Nederland alleen. Dit komt omdat een deel van de noodstroomvoorziening en opvang van pieken gebeurt vanuit andere landen in Europa. Omdat het Europese stroomnet zo is verweven is het lastig een specifiek land aan te vallen.

Dit scenario kent zeer veel varianten, omdat het leverancierspad zeer uitgebreid kan zijn, inclusief sub-componenten, chipmakers, ontwerpers etc. Een alternatief aanvalspad is bijvoorbeeld dat de APT toegang krijgt tot (onder-)fabrikanten van hardware- of softwarecomponenten door het afpersen of omkopen van insiders. Tenslotte zijn ook andere schakels in het systeem voor een soortgelijke aanval te misbruiken, bijvoorbeeld EMS-systemen, cloud-platformen en marktsystemen.

Tegelijkertijd zijn aanvallen via bijvoorbeeld grote fabrikantportaal ook grensoverschrijdend. De SolarMAN case uit 2022 gaf meteen toegang tot bijna 1 miljoen installaties wereldwijd. De oorzaak: een per ongeluk publiek gelekt wachtwoord op *github* (DIVD, 2022). In Nederland alleen werden ongeveer 40.000 installaties getroffen. In Europa een totaal van 10GW.

Waar ligt de kern van dit probleem?

De kern van dit probleem ligt bij de betreffende geraakte entiteit in de supply-chain. Deze entiteit zal op enige manier (omkoping, hacking, juridische pressie, druk vanuit een statelijke actor) de backdoor, bewust of onbewust, in omloop gebracht hebben. In sommige gevallen had de betreffende fabrikant mogelijk meer of andere maatregelen moeten treffen. In andere gevallen had wellicht de inkoper meer (cybersecurity) eisen moeten stellen aan de ingekochte component en de fabrikant die deze componenten levert,

De aanwezigheid van een backdoor zelf kan overigens lange tijd onopgemerkt blijven. Het is mogelijk om onderzoek te doen naar de vraag of een systeem een backdoor bevat. Maar dit zal veelal een momentopname zijn, die bij een volgende firmware update tenietgedaan wordt.

Wat zijn de gevolgen voor de eindgebruikers?

Dit scenario is een van de scenario's met potentieel de meeste impact. De verstoringen kunnen zo groot zijn dat de regionale en zelfs landelijke stroomvoorziening (tijdelijk) onderuitgaat. Zowel de eigenaren van zonnestroominstallaties als andere burgers in de regio die getroffen is zullen zonder stroom zitten.

De potentiële directe en indirecte gevolgen die eerder beschreven zijn (sectie 5.2), in de vorm van economische, fysieke en maatschappelijke schade, zijn bij dit scenario allemaal van toepassing.

Wie had dit kunnen voorkomen?

In beginsel hadden de verschillende landen die een rol spelen kunnen proberen om het conflict niet te laten escaleren tot het punt dat er cyberwapens ingezet worden. De realiteit is natuurlijk dat dit soms wel gebeurt.

De verschillende fabrikanten in de keten kunnen ieder voor zich proberen zich zo goed mogelijk te verdedigen en te proberen hun processen en methodes zo in te richten dat met name de grootschalige simultane exploitatie van de zonnepanelen installaties onmogelijk is. Voorkomen dat een statelijke actor binnendringt is zeer moeilijk. Daarom wordt het aangeraden om ook te kijken naar mogelijkheden om de impact te verkleinen, door technische beperkingen wanneer een dergelijke situatie zich wel voor zou doen.

Wat zijn de gevolgen voor anderen?

De gevolgen van dit scenario zijn onder meer het kunnen op- en afschakelen van in potentie >3GW vermogen - de genoemde grens voor de stabiliteit van het netwerk. Ook zou een actor die via deze weg in staat is om de elektrische parameters aan te passen langdurige schade aan kunnen brengen aan delen van het elektriciteitsnet. Dat kan bijvoorbeeld door een groot aantal zekeringen af te laten gaan die handmatig hersteld moeten worden.

In een dergelijke crisissituatie is het verder moeilijk te voorspellen wat de gevolgen exact zullen zijn. Veel van de Nederlandse kritieke infrastructuur zal door een dergelijke stroomstoring worden geraakt. Ook de secundaire gevolgen (zie 5.2 voor een aantal concrete voorbeelden) van een grootschalige stroomstoring moeten niet onderschat worden.

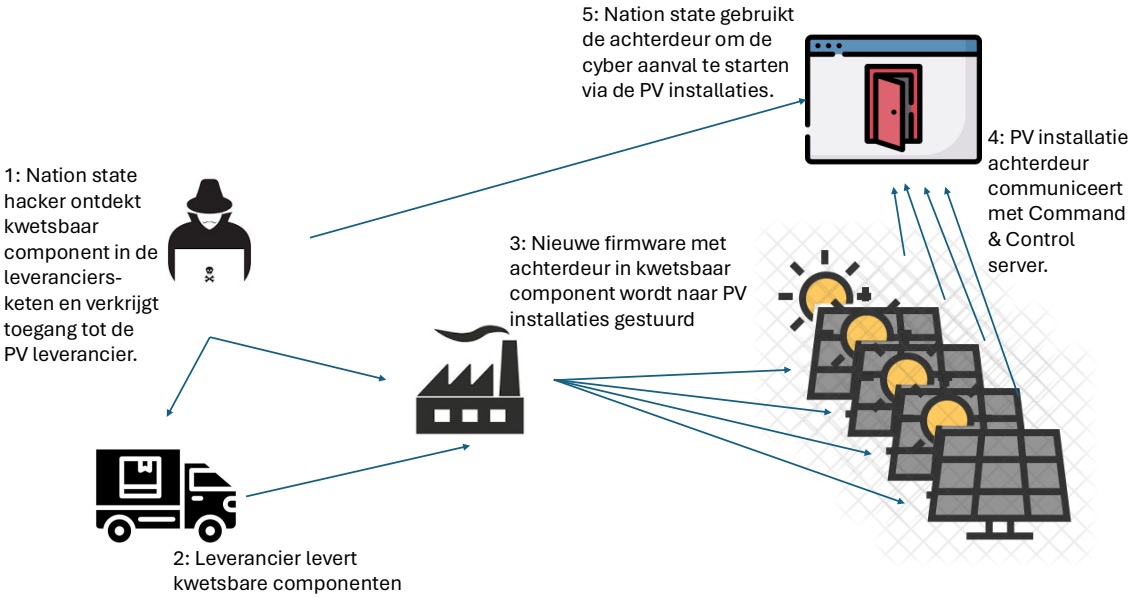
Hoewel onder meer ziekenhuizen en sommige bedrijven eigen noodstroomvoorzieningen hebben, zal de impact erg merkbaar zijn in alle getroffen regio's. Daarnaast zijn noodstroomvoorzieningen ook altijd bedoeld om tijdelijk stroom te kunnen leveren. Als door de aanval sprake is van langdurige stroomstoringen, zal de situatie moeilijker worden.

Naast alle directe en secundaire gevolgen, zal de inzet van een dergelijk cyberwapen op langere termijn ook serieuze gevolgen hebben op vlak van de geopolitiek en de onderlinge relatie tussen landen.

Schematische weergave

Hoewel niet alle dreigingsactoren hetzelfde doel van maatschappelijke verstoring voor ogen zullen hebben, zijn er diverse supply-chain aanvallen denkbaar binnen de zonnesector. Andere actoren zullen dergelijke toegang wellicht gebruiken om een ransomware-achtig verdienmodel in te zetten zoals in scenario 1 geschetst werd. Een grote maatschappelijke verstoring kan daarbij als het ware "nevenschade" zijn, van hun werkelijke doel (geld verdienen). Voor de statelijke actoren is het verkrijgen van mogelijkheden om de vitale infrastructuur van een land te ontregelen echter een doel op zich. Het

daadwerkelijk activeren van een dergelijk cyberwapen hoeft lang niet altijd te gebeuren. Er kan ook simpelweg mee gedreigd worden in politieke onderhandelingen. Hieronder volgt een versimpelde schematische weergave van dit scenario.



Figuur 7: Schematische weergave van een mogelijke supply-chain aanval

9. Mitigerende maatregelen

Nu het aanvalsoppervlak en de gevolgen duidelijk zijn, is uiteraard de belangrijkste vraag: wat kunnen we hieraan doen? Deze sectie zal proberen die vraag te beantwoorden.

9.1. Context

Veel van de maatregelen die hier beschreven worden zijn gericht zijn op nieuwe systemen en maatregelen die de systemen in de toekomst veilig kunnen houden. Wel moet er nagedacht worden over de economische haalbaarheid, omdat veel aanvullende cybersecurity-eisen de business case negatief kunnen beïnvloeden. De noodzaak voor extra maatregelen, desnoods via wet- en regelgeving, wordt echter wel als prioriteit gezien door nagenoeg alle betrokkenen van dit onderzoek. Een gelijk speelveld met minimum eisen en concurrentiemogelijkheden op vlak van cybersecurity kan de situatie sterk verbeteren t.o.v. de huidige markt, die sterk gericht is op competitie in prijs.

De meeste maatregelen die hier beschreven worden gelden ook in vergelijkbare sectoren, zoals elektrische auto's, batterijen, EMS-systemen en andere slimme grootverbruikers. Het belang van een integrale aanpak is noodzakelijk, omdat de zonnesector slechts een deel van het geheel is. Ook zouden veel van de maatregelen het meeste effect hebben als deze op Europees niveau geïmplementeerd zouden worden. Op die manier kan meer druk op fabrikanten uitgeoefend worden om te voldoen aan de verschillende nationale belangen.

Het koppelen van specifieke maatregelen aan de verschillende scenario's en risico's is sterk afhankelijk van degene die de maatregel moet nemen. De verschillende entiteiten in de zonnesector spelen allemaal een rol. Voor deze analyse zijn daarom de verschillende maatregelen in verschillende categorieën opgedeeld.

9.2. Techniek

Technische maatregelen zijn zeer krachtig omdat ze eenvoudig zijn en bepaalde zaken kunnen afdwingen. Er zijn een groot aantal frameworks en standaarden waarin cybersecurity-eisen of richtlijnen benoemd staan die kunnen helpen om individuele componenten veilig te maken. Denk daarbij aan de MASVS voor mobiele applicaties, de ASVS voor webapplicaties en portalen en bijvoorbeeld het ETSI EN 303 645 of Common Criteria model voor slimme apparaten. Deze verschillende frameworks kunnen bijdragen aan een hoger beveiligingsniveau. Bij de keuze voor fabrikanten kan ook gestuurd worden op de aanwezigheid van bepaalde technische maatregelen. Ook zouden sommige technische maatregelen vastgelegd kunnen worden in de vorm van een technische standaard specifiek voor de PV-sector.

Om toch een aantal cruciale maatregelen te benoemen:

- Gebruik van veilige wachtwoorden en multifactorauthenticatie.
- Software en firmware beveiliging.
- Veilige communicatieprotocollen.
- Borging van technische maatregelen door uitvoer beveiligingstest.

Verdere details omtrent deze cruciale maatregelen kan gevonden worden in sectie "Niveau: Techniek" in het technische achtergronddocument.

9.3. Productieketens

Installateurs

Deze partijen spelen een zeer belangrijke rol in de configuratie van de installatie. Installateurs zijn echter wel afhankelijk van de geboden opties en mogelijkheden van andere fabrikanten. Belangrijke maatregelen voor deze partijen zijn:

- Eigen cybersecuritybewustzijn verhogen.
- Cybersecuritybewustzijn bij hun klanten verhogen.
- Installaties van een bepaalde grootte zouden gecertificeerd kunnen worden, waarbij cybersecurity-eisen meegenomen worden.
- Opleidingen voor installateurs zouden ook cybersecurity moeten bevatten.
- Fabrikanten van installaties zouden installateurs verder op kunnen leiden.
- Fabrikanten van installaties zouden hun producten alleen kunnen laten plaatsen door bewezen competente installateurs.

Hardware- en softwarefabrikanten

Diverse partijen leveren verschillende stukjes van de totale zonnepaneleninstallaties. Deze fabrikanten zullen hun eigen componenten moeten beveiligen en daarnaast de nodige security-informatie aan moeten leveren over hun componenten aan hun klanten. De belangrijkste maatregelen voor deze partijen zijn de volgende:

- Basisbeveiligingsmaatregelen implementeren op alle centrale portalen.
- Beveiligingsmaatregelen treffen op de firmware van de geleverde componenten.
- Bewustwording van eigen personeel en dreigingen uit de eigen supply-chain
- Controleslagen inbouwen in het ontwikkelproces.
- Voor ieder geleverd product een Hardware- of Software Bill of Materials hebben (SBOM: een soort ingrediëntenlijst met wat er precies in dit apparaat aan onderdelen en componenten gebruikt is).
- Standaardconfiguratie moet meteen de “veiligste” zijn. Alle externe communicatie-opties staan standaard uit.
- Lage verwachtingen neerleggen bij de consument voor het instellen van het product. Eventuele verwachting die er wel nog zijn moeten zeer eenvoudig uitgelegd worden en haalbaar zijn voor leken.
- Configuratie van een component op afstand alleen mogelijk maken met lokale toestemming van de eindgebruiker.
- Kritieke parameters nooit aanpasbaar maken.
- De belangrijkste instellingen moeten alleen gewijzigd kunnen worden door competente installateurs.
- Er zou een productcertificering ingezet kunnen worden om een gelijk speelveld te creëren en minder alleen op prijs te concurreren.
- Er kan een open standaard en universeel protocol gemaakt worden voor de zonnesector, vergelijkbaar met wat eerder gedaan is voor laadpalen en slimme meters. Hierdoor ontstaat meer interoperabiliteit en minder leverancier-specifieke afhankelijkheid.

Projectontwikkelaars en opdrachtgevers

Bij de bouw van zonneparken of grote *rooftop* projecten wordt door deze entiteit veelal een installateur in de arm genomen. Tot nog toe gebeurt dat voornamelijk op basis van wie het goedkoopst is en de mooiste features biedt. Er is geen eis of selectie op basis van security. De extra kosten voor een hoger cybersecurityniveau zullen de kans om dit soort projecten te winnen dus negatief beïnvloeden. Om die situatie te veranderen zouden de volgende maatregelen kunnen helpen:

- Er kunnen minimale cybersecurity-eisen afgedwongen worden in aanbestedingen, tenders en inkooptrajecten.

- Er kan gebruik gemaakt worden van een (te ontwikkelen) standaard met uniforme cybersecurity-eisen en -maatregelen.
- Er kan strenger geselecteerd worden op (cyber-)bekwame installateurs
- In de opleverfase kan er een onafhankelijke controle uitgevoerd worden op de installatie waarbij cybersecurity-eisen ook meegenomen worden.
- Er kunnen binnen de sector uniforme cybersecurityrichtlijnen gemaakt worden, zodat niet ieder voor zich eigen richtlijnen maakt. Dit biedt structureel duidelijkheid voor zowel installateurs als projectontwikkelaars.

Verdere details omtrent deze maatregelen kan gevonden worden in sectie “Niveau: Productieketens” in het technische achtergronddocument.

9.4. Overheid en toezichthouders

Gezien de grote impact van deze sector op de Nederlandse burgers is het van belang dat ook de overheid en relevante toezichthouders hun rol spelen om de cyberweerbaarheid van de sector te verbeteren. De belangrijkste maatregelen daarbij zijn:

Wetgeving en certificering

- Er komen al een aantal nieuwe wetten en eisen aan certificeringen aan die impact gaan hebben op deze sector en de cybersecurity moeten gaan verbeteren (een uitgebreide lijst is te vinden in het technische achtergronddocument en in het recente rapport van solar power europe (SolarPower Europe, 2024)). Hoe deze in de praktijk geïmplementeerd gaan worden en hoe dit de situatie daadwerkelijk gaat verbeteren is nu nog niet duidelijk. Meer maatregelen of wetgeving voorstellen is op dit moment dan ook niet wenselijk.
- Het toetsen of de reeds gemaakte regels (en aankomende regels) voldoende nageleefd worden en voldoende impact hebben is echter wel zeer zinvol.
- Gegeven de levensduur van de reeds geïnstalleerde systemen moet er rekening gehouden worden dat de geschetste problemen nog zeker 10-15 jaar zullen blijven bestaan.
- Vanuit de toezichthouder, NCSC en DTC zou via de grootste (NIS2) organisaties vanuit de “zorgplicht” verplichting gestuurd kunnen worden om de keten sterker te maken. Bijvoorbeeld door meer eisen te stellen, kennis te delen en te helpen in het bekwaam maken van de gehele keten.
- Communicatie vanuit overheid en toezichthouders over aankomende regelgeving moet verbeterd worden, zodat betreffende entiteiten niet voor verassingen komen te staan. Met name kleine partijen weten nu vaak niet eens van het bestaan van deze regelgeving.
- De sector zou periodiek gewezen moeten worden op de relevante bestaande en nieuwe maatregelen. Een lijst met specifieke relevante maatregelen is opgenomen in het technisch achtergronddocument.
- Er zou verduidelijking moeten komen over de mate waarin een hardware- en softwareleverancier aansprakelijk te stellen is voor gevolgschade door een gebrek aan cybersecurity.
- Partijen zoals het NCSC & DTC zouden hierbij en gerelateerd aan bovenstaande punten ook partijen kunnen adviseren en ondersteunen in het verhogen van de algehele digitale weerbaarheid van de sector.
- Er zou duidelijkheid moeten komen over wie er aansprakelijk gesteld kan worden wanneer er iets misgaat door een cybersecurity incident. Daarnaast zouden de verschillende entiteiten in de sector hier ook over voorgelicht moeten worden.

Standaarden

- Door een universele standaard te creëren en gebruik hiervan af te dwingen, zoals ook voor slimme meters en laadpalen gebeurd is kan security-by-design een centrale plek krijgen in de keten.
- Een specifieke poort met een open, universeel protocol om data uitwisseling mogelijk te maken, kan voorkomen dat, een zonnepark eigenaar volledig afhankelijk wordt van een specifieke leverancier en bijbehorende Fabrikantportalen.
- Toelating tot de Nederlandse markt zou middels een Algemene Maatregel van Bestuur kunnen worden beperkt tot zonnestroominstallaties die aan de relevante standaarden voldoen. Ook zou er eventueel via verzekeraars gestuurd kunnen worden op bepaalde cyberveilige systemen gezien de schade veelal geclaimd zal worden op bijvoorbeeld inboedel- of opstalverzekeringen.

Preventief scannen en detecteren

- Er zou door bepaalde entiteiten preventief scans gedaan kunnen worden om kwetsbare punten te identificeren.
- Er zou door slimme inzet van publiek beschikbare bronnen gemonitord worden of kwetsbare punten voor het publieke internet beschikbaar zijn.
- Er zou binnen de sector informatie gedeeld kunnen worden over indicaties dat een systeem aangevallen is.
- Er zouden zogenaamde “honeypots” (een soort val voor hackers, waardoor achterhaald kan worden of er een aanval plaats vindt en hoe de aanval precies uitgevoerd wordt) ingezet kunnen worden om aanvallen in een vroegtijdig stadium te detecteren.
- Er kan actief onderzoek gedaan worden naar zwakheden in zonnestroominstallaties met een dominant marktaandeel.
- Alarmmeldingen zouden gegeven kunnen worden aan de sector door de relevante entiteiten.

Soevereiniteit van data en beheer op afstand

- De Nederlandse en Europese politiek zou beargumenteerd een keuze moeten maken over hoeveel van de stroomopwekkende systemen van buiten Europa beheerd zouden mogen worden en of daar nog aanvullende eisen aan gesteld zouden moeten worden.
- De residentiële installaties van een specifiek merk, zouden gezamenlijk opgeteld kunnen worden om een virtueel equivalent van deze “energiecentrale” te maken. En op die manier te bepalen of aanvullende eisen wellicht ook voor specifieke fabrikanten of centrale portalen moeten gelden.

Verdere details omtrent deze maatregelen kan gevonden worden in sectie “Niveau: Overheid en Toezichthouders” in het technische achtergronddocument.

9.5. Brancheorganisaties en ISAC

Naast de eerdergenoemde entiteiten is er nog een aantal ander overkoepelende organen die kennis delen en ‘*best practices’* uitwisselen. Deze kunnen ook een rol spelen bij de verbetering in de sector. De volgend maatregelen zouden getroffen kunnen worden:

Brancheorganisaties

- Er kan positieve aandacht besteed worden aan goede voorbeelden na onafhankelijk onderzoek in samenwerking met partijen zoals de Consumentenbond, Milieu Centraal of Topsector Energie.
- Er zou een duidelijk zichtbaar keurmerk dat begrijpelijk is voor consumenten opgezet kunnen worden. Dat keurmerk zou toegepast kunnen worden op individuele componenten, complete installaties of op specifieke installateurs.

- Veel van de bij “installateurs” genoemde punten voor verbetering zouden breed opgepakt en gedreven kunnen worden via reeds bestaande brancheorganisaties.

Kennisdeling en information ISAC

- Gegeven de specifieke uitdagingen in de zonnesector zal het vermoedelijk beter zijn om een eigen ISAC (Information Sharing and Analysis Centre) te vormen.
- Bestaande werkgroepen zoals bijvoorbeeld Holland Solar zouden meer gebruikt moeten worden om belangrijke informatie voor de sector te delen. Denk daarbij bijvoorbeeld ook aan aankomende wet- en regelgeving of initiatieven om standaarden te ontwikkelen.
- Een actievere rol van brancheorganisaties om ook “niet-leden” te bereiken met belangrijke informatie is wenselijk. Veelal zijn de “achterblijvers” geen lid van dergelijke branchеverenigingen.

9.6. Eindgebruikers en afnemers

Consumenten en zakelijke gebruikers hebben natuurlijk zelf ook een rol te spelen in het veilig houden van de installatie. Tegelijkertijd kun je niet verwachten dat iedereen een IT of cybersecurity expert is. Het is dan ook belangrijk dat verschillende entiteiten de consumenten voldoende informeren, adviseren en ontzorgen. De volgende belangrijke maatregelen kunnen getroffen worden:

Het helpen van de Consumenten

- Bewustwording van de mogelijke risico’s (bijvoorbeeld op vlak van wachtwoorden) en de eigen rol hierin door advies en informatie vanuit de installateurs.
- Installatiehandleidingen zouden realistische aanbevelingen moeten bevatten die uitvoerbaar zijn voor leken. Zaken zoals een apart virtueel netwerk inrichten specifiek voor het apparaat is voor de meeste consumenten een onmogelijke opgave.
- De installateur zou een adviserende rol naar de consument moeten hebben, waarbij een elektrisch veilige en cyber veilige installatie wordt geplaatst bij de consument. De kosten die dit met zich meebrengt kunnen daardoor voor de consument inzichtelijk worden gemaakt.
- Adviezen van de brandweer over hoe om te gaan en waar te plaatsen van de zonnestroominstallatie moeten worden duidelijk gemaakt aan de consument en installateurs en ook gehonoreerd worden door de installateurs.
- Er zouden service contracten aangeboden kunnen worden aan consumenten voor periodieke controle en updates.
- De stappen voor veilige basisconfiguratie kunnen door een installateur samen met de consument doorlopen worden.
- De koppeling van het systeem met het internet of cloud-diensten kan als keuze in plaats van verplichting bij de consument neergelegd worden. Informatie verkrijgen over de opwek kan vaak op meer manieren, bijvoorbeeld via waardes afkomstig uit de slimme meter of door gebruik van de lokale interface.

Zakelijk

- Vergroten van bewustwording van cyberveiligheid in de algemene zin.
- Netwerksegmentatie toepassen om risico’s te verkleinen.
- Toegang op afstand beperken en sterk beveiligen.
- Mogelijkheden inbouwen om connectie met externe fabrikantportalen te beperken of alleen open te stellen wanneer nodig.
- Vanaf een bepaalde geaggregeerde grootte zou voldaan moeten worden aan bepaalde cybersecurity eisen.

- Ook zou er voor zonneparken en zakelijke gebruikers onder die grootte een set aan minimale cybersecurity-richtlijnen en basismaatregelen afgesproken moeten worden. Dit moet ook gelden voor reeds bestaande parken.
- Er moet niet alleen gekeken worden naar de impact op het eigen bedrijf maar ook nadruk gelegd worden op de impact die het heeft op andere sectoren in de keten.
- Opdrachtgevers moeten cybersecurity meenemen in ontwerpeisen, aanbestedingseisen, uitbesteding en overige partners in de keten.

Verdere details omtrent deze maatregelen kan gevonden worden in sectie “Niveau: Eindgebruikers” in het technische achtergronddocument.

10. Conclusie

De conclusie van dit onderzoek is dat er in de zonnestroomsector in Nederland een significant aanvalsoppervlak is en dat dit zich in de toekomst vooral nog verder zal uitbreiden. De opwekking van zonnestroom wordt steeds de-centraler, wordt steeds slimmer en vergt steeds meer connecties met internet en diensten. Ook blijkt dat cascade-effecten door de complexiteit erg moeilijk op detailniveau te voorspellen zijn. Wanneer gekeken wordt naar de gehele keten zijn er diverse aanvalsscenario's te bedenken waarmee grootschalige aanvallen op de zonnesector en indirect daarmee op de energiesector mogelijk zijn.

De gevolgen van zo'n cyberaanval zijn potentieel desastreus en kunnen veel economische, fysieke en maatschappelijke schade met zich meebrengen. Hoeveel schade een cyberaanval precies aanricht en bij wie, zal afhankelijk zijn van de aanvaller en diens achterliggende doel. Tot nog toe is er vanuit dreigingsbeelden bekend dat er veel aandacht gegaan is naar de energiesector als geheel. Er is echter nog weinig motivatie geweest om specifiek de zonnesector aan te vallen. In de praktijk zien we echter dat het wel degelijk mogelijk zou zijn om met een gerichte aanval op de zonnesector de energiesector als geheel te raken.

Om succesvolle cyberaanvallen te voorkomen en de impact van een eventuele succesvolle aanval te verkleinen zullen vrijwel alle entiteiten die deel uitmaken van de zonnesector actie moeten ondernemen. Deze gedeelde verantwoordelijkheid zal niet eenvoudig te realiseren zijn, maar is wel noodzakelijk om op de lange termijn de stabiliteit van het stroomnet te kunnen garanderen. We willen de betrokkenen in de sector dan ook aanmoedigen tot samenwerking, zodat de belangen van alle betrokken partijen gewaarborgd kunnen worden in de sector als geheel. Daarbij valt ook op dat tijdens dit onderzoek verschillende deelnemers naar aanleiding van de gesprekken zelf aangaven aanvullende maatregelen te zullen nemen binnen de eigen organisatie. Dit onderstreept nogmaals het belang van een goede samenwerking en kennisdeling tussen de verschillende entiteiten.

Er zijn dan ook nog diverse oplossingen aangedragen, zoals het ontwikkelen van standaarden en universele protocollen. Waar mogelijk zouden deze middels consortia en met reeds bestaande samenwerkingsverbanden ontwikkeld moeten worden. Adoptie hiervan zal wellicht gesubsidieerd moeten worden om in de praktijk een zo hoog mogelijke adoptiegraad te krijgen.

Tot slot is duidelijk geworden dat diverse geïdentificeerde problemen en maatregelen niet alleen van toepassing zijn op de zonnesector, maar ook daarbuiten. Denk aan EMS-systemen, batterij systemen, laadpalen en andere slimme grootverbruikers. Er zijn al vergelijkbare onderzoeken gedaan naar deze specifieke delen, maar een overkoepelende aanpak ontbreekt. En dat terwijl vanuit al deze deelmarkten slimme connecties met elkaar gemaakt worden, vele startups de markt betreden en er alleen maar meer koppelingen en afhankelijkheden bijkomen. Het is daarom raadzaam om naast de specifieke onderzoeken ook te komen tot een integrale aanpak die zich richt op toekomstbestendigheid van al deze slimme systemen in het geheel. Daarnaast zouden ook specifiek de (H)EMS-systemen nog goed onderzocht moeten worden omdat deze de verschillende energietransitie gerelateerde apparatuur allemaal aan elkaar koppelt om efficiënt met de stroom om te gaan, maar daarmee ook een potentieel single point of failure is voor al deze apparatuur.

11. Referenties en bronnen

Brumfield, C. (2024, May 23). *Hijack of monitoring devices highlights cyber threat to solar power infrastructure*. Retrieved from CSO: https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html

CBS. (2024, June 17). *Zonnestroom; vermogen en vermogensklasse, bedrijven en woningen, regio*. Retrieved from www.cbs.nl: https://www.cbs.nl/nl-nl/cijfers/detail/85005NED

Cloudflare. (2024, June 20). *What is the Mirai botnet*. Retrieved from Cloudflare.com: https://www.cloudflare.com/en-gb/learning/ddos/glossary/mirai-botnet/

Counter threat unit research team. (2023, December 7). *Iranian Cyber Av3ngers compromise unitronics systems*. Retrieved from Secureworks.com: https://www.secureworks.com/blog/iranian-cyber-av3ngers-compromise-unitronics-systems

DIVD. (2022, July 24). *Solarman backend administrator account*. Retrieved from csirt.divd.nl: https://csirt.divd.nl/cases/DIVD-2022-00009/

Dutch New Energy Research en Solar 365. (2024, February 1). *Nationaal Solar Trendrapport.* Retrieved from Solarsolutions.nl: https://www.solarsolutions.nl/good-solar-solutions/_SiteFiles/file/2024-solar-trendrapport-web.pdf

Energie Opwek. (2024, June 26). *Nationaal energie dashboard*. Retrieved from energieopwek.nl: https://energieopwek.nl/en/

Fairley, P. (2015, February 5). *800,000 Microinverters remotely retrofitted on Oahu- in One Day*. Retrieved from spectrum.ieee.org: https://spectrum.ieee.org/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu

Gastel, E. v. (2024, March 3). *Nederland passeert grens van 3 miljoen installaties met zonnepanelen*. Retrieved from Solar magazine: https://solarmagazine.nl/nieuws-zonne-energie/i37036/copyright-auteursrecht

NOS. (2015, Maart 27). *Grote Stroomstoring TenneT legt Noord-Holland plat*. Retrieved from nos.nl: https://nos.nl/nieuwsuur/artikel/2027234-grote-stroomstoring-tennet-legt-noord-holland-plat

Rijksinspectie Digitale Infrastructuur. (2023, May 30). *Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen*. Retrieved from RDI.nl: https://www.rdi.nl/actueel/nieuws/2023/05/30/omvormers-kunnen-storing-veroorzaken-en-zijn-vaak-makkelijk-te-hacken

Secura. (2024, July 1). *RVO.nl*. Retrieved from PLACEHOLDER: www.rvo.nl/PLACEHOLDER

Security.nl. (2022, July 25). *Miljoen omvormers zonnepanelen via gelekt wachtwoord kwetsbaar voor sabotage*. Retrieved from Security.nl: https://www.security.nl/posting/762224/Miljoen+omvormers+zonnepanelen+via+gelekt+wachtwoord+kwetsbaar+voor+sabotage

Sluijters, S. (2022, Januari 17). *Nederland Europese koploper zonne-energie*. Retrieved from ChangeInc: https://www.change.inc/energie/nederland-europese-koploper-zonne-energie-37603

SolarPower Europe. (2024, July 12). *Setting a Harmonised Cybersecurity Baseline for Solar PV*. Retrieved from https://www.solarpowereurope.org: https://www.solarpowereurope.org/advocacy/position-papers/setting-a-harmonised-cybersecurity-baseline-for-solar-pv

TNO. (2019, Maart 13). *publications.tno.nl*. Retrieved from TNO-2019-R10287: https://publications.tno.nl/publication/34633946/bhxqSn/TNO-2019-R10287.pdf

TNO, C. v. (2024). *Eindadvies Cyberzon.* TKI urban energy.

Wikipedia. (2024, Juni 28). *Clauscentrale*. Retrieved from Wikipedia: https://nl.wikipedia.org/wiki/Clauscentrale

12. Colofon

Deze rapportage is tot stand gekomen dankzij inbreng van experts en ervaringsdeskundigen vanuit diverse partijen in de zonne-energiesector, energieleveranciers, netbeheerders, brancheorganisaties, overheden en kennispartijen.

Opgesteld door:

- Frank Ruedisueli, Secura
- Willem Westerhof, Secura
- Ralph Moonen, Secura
- Sjoerd Peerlkamp, Secura

In opdracht van:

- Jorn Peeters, Rijksdienst voor Ondernemend Nederland
- Karel Haverkorn, Rijksdienst voor Ondernemend Nederland
- Soe van Dijk, Topsector Energie Digitalisering
- Pim Vork, TKI Urban Energy

Speciale dank aan de volgende geraadpleegde personen en organisaties:

- Digital Trust Center
- Gerben Broenink, TNO
- Jaap van Eijk, Fronius
- Jeroen van der Molen, Sunergetic
- John van Vugt, Techniek Nederland
- Karel Lambers, Everday
- Karl van de Vijver
- Maaike Beenes, Holland Solar
- Mathijs Arends, Groendus
- Mike Scharrenberg, Liander
- Nationaal Cyber Security Centrum
- Peter Baard, NV RENDO
- Philipp Rechbecher, Fronius
- Safey Attia, Gutami
- Sander Dannenberg, Novar
- SMA
- Stephan Gerling, GeConIT
- WiththeGrid

Rechten en vrijwaring:

Topsector Energie en RVO

De Rijksdienst voor Ondernemend Nederland (RVO) stimuleert duurzaam, agrarisch, innovatief en internationaal ondernemen. Met subsidies, het vinden van zakenpartners, kennis en het voldoen aan wet- en regelgeving. RVO werkt in opdracht van ministeries en de Europese Unie. RVO is een onderdeel van het ministerie van Economische Zaken. TKI Urban Energy is een onderdeel van de Topsector Energie (TSE) en stimuleert bedrijven, kennisinstellingen, maatschappelijke organisaties en overheden om samen te werken op het gebied van energie-innovatie in de gebouwde omgeving. Het TSE Programma Digitalisering richt zich op de digitalisering van het energiesysteem, met aandacht voor kansen voor innovatie met digitale technologieën evenals reflectie op randvoorwaarden zoals cyberweerbaarheid.

RVO, TKI Urban Energy en TSE Digitalisering bevorderen samen onderzoek naar cybersecurity binnen de context van de transitie naar een duurzaam, betrouwbaar en betaalbaar energiesysteem. Dit doen we door initiatieven financieel te steunen, betrokken partijen bij elkaar te brengen en kennis te delen. Met deze input adviseert de Topsector Energie de overheid bij haar beleidsontwikkeling, bedrijven bij hun innovatieaanpak en kennisinstellingen bij hun onderzoeksvragen.

Wil je naar aanleiding van deze publicatie in contact komen met de opdrachtgevers, neem dan contact op met:

Topsector Energie Digitalisering
Soe van Dijk
Soe.vandijk@topsectorenergie.nl

RVO
Jorn Peeters
Jorn.peeters@rvo.nl

Secura

Sinds 2000 helpt Secura bedrijven, (zorg-)organisaties en (lokale) overheden bij het identificeren, verminderen en voorkomen van IT-beveiligingsrisico's. Dit doen we door het uitvoeren van audits, beveiligingsonderzoeken en -beoordelingen, consultancy, penetratietests en certificering van producten en diensten. Met kantoren in Eindhoven en Amsterdam wordt de Benelux-markt bediend. In 2021 is Secura onderdeel van Bureau Veritas (BV) geworden, een wereldwijd actief bedrijf dat tests, inspecties en certificeringen uitvoert op veel gebieden. In 2024 is de servicelijn Secura International opgericht in samenwerking met Bureau Veritas om ook onze internationale klanten te helpen hun cyberweerbaarheid te vergroten.

Wil je naar aanleiding van deze publicatie in contact komen met Secura, neem dan contact op met:

Secura B.V.
Erwin Jansen, Manager Marktgroep Public
erwin.jansen@secura.com